AUTHENTICATED
U.S. GOVERNMENT
INFORMATION
GPO

SEXUAL EXPLOITATION OF CHILDREN OVER THE INTERNET: HOW THE STATE OF NEW JERSEY IS COMBATING CHILD PREDATORS ON THE INTERNET

HEARING

BEFORE THE

SUBCOMMITTEE ON OVERSIGHT AND INVESTIGATIONS

OF THE

COMMITTEE ON ENERGY AND COMMERCE
HOUSE OF REPRESENTATIVES

ONE HUNDRED NINTH CONGRESS

SECOND SESSION

JULY 10, 2006

Serial No. 109-122

Printed for the use of the Committee on Energy and Commerce

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

U.S. GOVERNMENT PRINTING OFFICE

30-531PDF WASHINGTON : 2006

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) 512-2250 Mail: Stop SSOP, Washington, DC 20402-0001

COMMITTEE ON ENERGY AND COMMERCE

JOE BARTON, Texas, *Chairman*

RALPH M. HALL, Texas
MICHAEL BILIRAKIS, Florida
Vice Chairman
FRED UPTON, Michigan
CLIFF STEARNS, Florida
PAUL E. GILLMOR, Ohio
NATHAN DEAL, Georgia
ED WHITFIELD, Kentucky
CHARLIE NORWOOD, Georgia
BARBARA CUBIN, Wyoming
JOHN SHIMKUS, Illinois
HEATHER WILSON, New Mexico
JOHN B. SHADEGG, Arizona
CHARLES W. "CHIP" PICKERING, Mississippi
Vice Chairman
VITO FOSSELLA, New York
ROY BLUNT, Missouri
STEVE BUYER, Indiana
GEORGE RADANOVICH, California
CHARLES F. BASS, New Hampshire
JOSEPH R. PITTS, Pennsylvania
MARY BONO, California
GREG WALDEN, Oregon
LEE TERRY, Nebraska
MIKE FERGUSON, New Jersey
MIKE ROGERS, Michigan
C.L. "BUTCH" OTTER, Idaho
SUE MYRICK, North Carolina
JOHN SULLIVAN, Oklahoma
TIM MURPHY, Pennsylvania
MICHAEL C. BURGESS, Texas
MARSHA BLACKBURN, Tennessee

JOHN D. DINGELL, Michigan
Ranking Member
HENRY A. WAXMAN, California
EDWARD J. MARKEY, Massachusetts
RICK BOUCHER, Virginia
EDOLPHUS TOWNS, New York
FRANK PALLONE, JR., New Jersey
SHERROD BROWN, Ohio
BART GORDON, Tennessee
BOBBY L. RUSH, Illinois
ANNA G. ESHOO, California
BART STUPAK, Michigan
ELIOT L. ENGEL, New York
ALBERT R. WYNN, Maryland
GENE GREEN, Texas
TED STRICKLAND, Ohio
DIANA DEGETTE, Colorado
LOIS CAPPS, California
MIKE DOYLE, Pennsylvania
TOM ALLEN, Maine
JIM DAVIS, Florida
JAN SCHAKOWSKY, Illinois
HILDA L. SOLIS, California
CHARLES A. GONZALEZ, Texas
JAY INSLEE, Washington
TAMMY BALDWIN, Wisconsin
MIKE ROSS, Arkansas

BUD ALBRIGHT, *Staff Director*
DAVID CAVICKE, *General Counsel*
REID P. F. STUNTZ, *Minority Staff Director and Chief Counsel*

SUBCOMMITTEE ON OVERSIGHT AND INVESTIGATIONS

ED WHITFIELD, Kentucky, *Chairman*

CLIFF STEARNS, Florida
CHARLES W. "CHIP" PICKERING, Mississippi
CHARLES F. BASS, New Hampshire
GREG WALDEN, Oregon
MIKE FERGUSON, New Jersey
MICHAEL C. BURGESS, Texas
MARSHA BLACKBURN, Tennessee
JOE BARTON, Texas
(EX OFFICIO)

BART STUPAK, Michigan
Ranking Member
DIANA DEGETTE, Colorado
JAN SCHAKOWSKY, Illinois
JAY INSLEE, Washington
TAMMY BALDWIN, Wisconsin
HENRY A. WAXMAN, California
JOHN D. DINGELL, Michigan
(EX OFFICIO)

CONTENTS

	Page
Testimony of:	
Christie, Hon. Christopher J., United States Attorney, District of New Jersey, U.S. Department of Justice	8
Fitzpatrick, Hon. Michael, Member, U.S. House of Representatives	27
Rodgers, Frank, Lieutenant Colonel, New Jersey State Police	35
Ritter, Anthony, Lieutenant, New Jersey State Police	40
Forrest, Esq., Wayne J., Somerset County Prosecutor, Office of the Somerset County Prosecutor, State of New Jersey	47
Banks, Sergeant, Office of the Prosecutor, Union County, State of New Jersey	55
Livingston, David S., Superintendent of Schools, Somerset County, New Jersey	75
Aftab, Parry, Executive Director, WiredSafety	81
Sullivan, Shannon, Teen Angel, WiredSafety	116
Hahn, Samantha, i-Mentor, i-Safe America	134

SEXUAL EXPLOITATION OF CHILDREN OVER THE INTERNET: HOW THE STATE OF NEW JERSEY IS COMBATING CHILD PREDATORS ON THE INTERNET

MONDAY, JULY 10, 2006

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

The subcommittee met, pursuant to notice, at 10:30 a.m., in Conference Center Room A of the Raritan Valley Community College, Hon. Ed Whitfield (Chairman) presiding.

Members present: Representatives Whitfield and Ferguson.

Staff present: Mark Paoletta, Chief Counsel for Oversight and Investigations; Kelli Andrews, Counsel; Karen Christian, Counsel; Ryan Ambrose, Legislative Clerk; and David Nelson, Minority Investigator.

MR. WHITFIELD. I would like to call this hearing to order and I certainly want to thank all of you for attending today. The Energy and Commerce Committee and the Subcommittee on Oversight and Investigation are convening this hearing in New Jersey on the Sexual Exploitation of Children over the Internet. The subcommittee has held four hearings on this subject. We have heard testimony from victims of Internet child pornography, State and Federal law enforcement agents, safety and Internet education experts and Internet service providers about the dangers the Internet can pose to children.

While Federal law enforcement agents actively investigate and pursue online predators, 70 percent of the investigations take place at the State and local level through the efforts of the State Internet Crimes Against Children Task Force and local police officers and investigators and prosecutors. For this reason, the subcommittee thought it would be important to have a hearing where we would focus on local efforts to deal with this significant problem. Like every other State, New Jersey is not immune from the dangers that the Internet presents to children. Today we will hear testimony from witnesses who work each day to combat child pornography and to keep New Jersey's children safe from predators who seek to use the Internet to exploit them.

These hearings that we have had have been quite startling to all of us, to recognize and be aware of the dangers that are lurking out there for

our young people who are on the Internet and come in contact with some very unsavory characters. Today we are going to hear from the United States Attorney for the District of New Jersey, Chris Christie, about the cases brought by his office against child predators. Particularly, we will be interested in his RegPay case, which was a real breakthrough; I guess the first international breakthrough in this area. We will also hear from the New Jersey State and local police officers about how they developed their investigations against individuals who exploit children on the Internet and the challenges they face when they attempt to bring these criminals to justice.

Our subcommittee's hearings have shown that every effort must be made to support law enforcement efforts in the war against child pornography, but they also have shown that we will not win this war unless we educate parents, teachers and children about Internet safety. Witnesses have repeatedly told our subcommittee that children often are not able and do not appreciate the risk posed to them when they meet and communicate over the Internet with strangers.

Two of our witnesses today, i-Safe Mentor, Samantha Hahn, and WiredSafety Teen Angel, Shannon Sullivan, have been trained to talk to their friends and fellow students about Internet safety. We look forward to learning what they believe is the most effective way to teach children to protect themselves against online predators. Samantha and Shannon are joined by Superintendent David Livingston of the Somerset County Schools, who will testify about how schools in his district are addressing Internet safety issues, as well as problems related to social networking sites, cyber bullying and online predators.

We will also be joined today by Congressman Michael Fitzpatrick of Pennsylvania. Congressman Fitzpatrick has introduced a bill, H.R. 5319, entitled "The Deleting Online Predators Act," which requires schools and libraries to use technology on their computers that prevent students from accessing social networking sites, and we look forward to Mr. Fitzpatrick's testimony when he arrives.

And finally, I want to thank my colleague, Mike Ferguson, who is a member of the Energy and Commerce Committee and certainly a member of the Oversight and Investigations Subcommittee. He has been a real leader in this effort to address the dangers facing our children on the Internet and I know that he shares our interest in this issue. He has been dedicated to doing whatever can be done to keep the Internet safe for children and to ensure that criminals who use the Internet to prey on our children are found and prosecuted. And I want to thank him for arranging for this hearing today and convincing us to come to New Jersey to learn what, specifically, law enforcement prosecutors and others are doing in this area about this important issue.

So I want to thank all of you for being here and at this time I will recognize Mr. Ferguson for his opening statement.

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

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

Today, the Committee on Energy and Commerce, Subcommittee on Oversight and Investigations, is convening a hearing in New Jersey on the sexual exploitation of children over the Internet.

Already, this subcommittee has held four hearings on this subject. We have heard testimony from victims of Internet child pornography, state and federal law enforcement agents, safety and Internet education experts, and Internet Service Providers about the dangers the Internet can pose to children.

From these hearings, this subcommittee has learned that while federal law enforcement agents actively investigate and pursue online predators, seventy percent of the investigations of these criminals take place at the state and local level through the efforts of the state Internet Crimes Against Children Task Forces, or "ICACs," and local police officers. For this reason, the subcommittee thought it was important to dedicate a hearing to how the war against child pornography and the online exploitation of children is being fought on the ground, by state and local law enforcement agents.

Like every other state in the nation, New Jersey is not immune from the dangers the Internet presents to children. Today we will hear testimony from witnesses who work each day to combat child pornography and to keep New Jersey's children safe from predators who seek to use the Internet to exploit them. We will hear from the United States Attorney for the District of New Jersey, Chris Christie, about the cases brought by his office against child predators. We will also hear from New Jersey state and local police officers about how they develop their investigations against individuals who exploit children over the Internet, and the challenges they face when they attempt to bring these criminals to justice. I look forward to learning whether the witnesses believe they have the resources they need to not only fight the war against child pornography on the Internet, but to win it. As this subcommittee held a hearing only two weeks ago with Internet Service Providers and social networking sites, I also look forward to learning your thoughts about the industry's efforts to combat online child pornography and whether you believe more should be required of them. Finally, because the vast majority of cases against online predators are prosecuted at the state and local level, I am interested to learn if additional federal resources would help facilitate your investigations and prosecutions.

Just as our subcommittee's hearings have shown that every effort must be made to support law enforcement's efforts in the war against child pornography, they have also shown that we will not win this war unless we educate parents, teachers, and children about Internet safety. Witnesses have repeatedly told this subcommittee that children often are not able to appreciate the risk posed to them when they meet and communicate over the Internet with a stranger. Two of our witnesses today, i-Safe mentor Samantha Hahn and Wired Safety Teen Angel Shannon Sullivan, have been trained to talk to their friends and fellow students about Internet safety. I look forward to learning what they believe is the most effective way to teach children to protect themselves against online predators. Samantha and Shannon are joined by Superintendent David Livingston of the Somerset County Schools, who will testify about how schools in his district are addressing Internet safety issues as well as problems related to social networking sites, cyber bullying, and online predators.

We are also joined today by Congressman Michael Fitzpatrick of Pennsylvania. Congressman Fitzpatrick has introduced a bill, H.R. 5319, the Deleting Online Predators Act. H.R. 5319 requires schools and libraries to use technology on their computers that prevents students from accessing social networking sites. Thank you, Congressman Fitzpatrick, for making the trip to appear before us this morning to discuss your efforts to combat online predators.

Finally, I would like to thank my colleague, Mike Ferguson, for welcoming us to his district. I know that Congressman Ferguson shares my interest in this issue, and that he is dedicated to doing whatever he can to keep the Internet safe for children and to ensure that the criminals who use the Internet to prey on children are found and prosecuted.

Thank you.

MR. FERGUSON. Thank you, Mr. Chairman. Thank you for being here, very much for your welcome here in New Jersey. I am delighted to have you here and really pleased that we could do this hearing here in New Jersey. I also want to thank--we have several panels of really excellent witnesses. I am delighted that they are all here. I particularly appreciate the U.S. Attorney being here today and our Somerset County Prosecutor, Wayne Forrest. I appreciate you and all the other panelists who are going to join us here today. I think this is going to prove to be an excellent line-up for shedding some light on how we can combat this problem here in New Jersey.

I appreciate very much and want to personally commend some of our other panelists for the work that they are doing every day to combat this issue in our families and in our communities. Throughout the course of the past few months, we in Congress have held several hearings on this topic. We have heard from law enforcement, from Internet service providers, from social networking sites, from Internet education groups, Federal officials from the Department of Justice and other Federal agencies, as well as some of the victims themselves. But no matter how many hearings we have on this topic, it never gets any easier to hear about and it still shocks and sickens every one of us.

The National Center for Missing and Exploited Children reports that 39 percent of persons caught with images of child sexual abuse had images of children younger than 6 years old, and 19 percent of these people caught had images of children under 3 years old. In all of my years, as a Member of Congress, as an educator and most importantly, as a parent, I have never been so disturbed by a topic that we have considered. It is beyond comprehension that we, as a society, have allowed this industry to flourish, sometimes even within the confines and protection of our own homes. And it is our responsibility, as lawmakers, as parents, as educators, and law enforcement, to do everything possible to let our children know that they are safe and that they will be protected at all costs.

I am not just a Member of Congress and a public servant; I am also a parent with four young kids. Like millions of other families, my wife and I talk to our kids about the great opportunities for fun and learning that the Internet has to offer, but we also need to protect our children from those who use the Internet to try and harm them. The private sector and government and law enforcement must work together to ensure that we all have the necessary tools to keep our children safe.

This issue is gruesome, it is heart wrenching, and it is disturbing, but it is not one that we can ignore. The Internet can be an extraordinary tool for our children, but it also harbors dangers that we must be aware of. The predators that lurk on the Internet take advantage of children in the cruelest of ways; by earning their trust and stealing their innocence, and this leaves a pain that no child should ever have to endure. I am proud to say that New Jersey has strong law enforcement programs directed toward, dedicated to rooting out Internet predators.

Today we will hear some of the success stories of the New Jersey Internet Crimes Against Children Task Force, as well as the collaborative efforts with other ICACs across the country. Our educators have also made an effort to teach our children about the dangers of the Internet. Law enforcement and local schools have been teaming up to educate both children and parents on how to safely use the World Wide Web. Organizations such as i-Safe and WiredSafety have made it their mission to educate children about how to use the Internet safely and what warning signs to look out for.

Specifically, i-Safe has educated over 43,000 students on Internet safety and implemented 30 parent education programs in New Jersey alone. I commend these organizations for their programs and sincerely hope they can continue in the future. I look forward to hearing from our witnesses today and I hope this hearing serves to further draw attention to this issue, especially in a State where we have so many good people working on behalf of our children.

Again, I want to thank you, Chairman Whitfield, for allowing us to bring the Congress to New Jersey today. I want to thank our witnesses for coming to the committee today and I particularly want to thank Raritan Valley Community College for so graciously hosting this field hearing today. I appreciate all of the efforts on their behalf and on behalf of the committee and the subcommittee staff for their work in pulling this hearing together.

MR. WHITFIELD. Mike, thank you very much and I will say that the interim president of Raritan Community College was here to greet us this morning and took us on a tour and we are all ready to move to New Jersey. But I appreciate your opening statement. At this time, we have four panels of witnesses today and at this time we will start with our

second panelist and that is the Honorable Christopher Christie, who is the U.S. Attorney for the District of New Jersey, U.S. Department of Justice. So if you wouldn't mind coming forward, Mr. Christie. I would mention to you that Oversight and Investigation, when we take testimony, we do it under oath and under the rules of the House and certainly the rules of the committee, you are entitled to legal counsel, but since you are a U.S. attorney, I assume you don't need legal counsel. But if you don't have any difficulty testifying under oath, would you stand up and I would like to swear you in.

[Witness sworn.]

MR. WHITFIELD. Thank you, Mr. Christie. You are now under oath and you are recognized for your 5-minute opening statement.

STATEMENT OF HON. CHRISTOPHER J. CHRISTIE, UNITED STATES ATTORNEY, DISTRICT OF NEW JERSEY

MR. CHRISTIE. Mr. Chairman, thank you for coming to New Jersey, Congressman Ferguson. Thank you for inviting me here today to speak about this very important topic. Let me say, first, that here in New Jersey we have enormously fruitful cooperative efforts that are going on between Federal, State, and local law enforcement. I am sure you will hear from my law enforcement partners on the State and local level a lot about that in the testimony that will follow mine. We have great cooperation, cases being done federally and on the State level, and they are decided on whether or not to do them federally or State based upon where we can get the best sentence, where we can get the best possible result. There are no egos involved, there are no turf battles over this and I am proud to say that in this State, everyone is cooperating very well because they see how important the problem is.

One particular investigation, which I think deserves note this morning, is the one you referred to in your opening remarks, Mr. Chairman, the RegPay investigation. That remains the first and I think, most successful international attack on child pornography here from the Department of Justice. And let me tell you how that began. It literally began by an assistant United States Attorney, in my office, coming into my office one day and saying to me I have a new idea about how to go after this child porn problem. And I think it is important to note how it began because it is just one dedicated assistant United States Attorney who had an idea, came to my office, sold me on the idea and we, then, went about getting Federal law enforcement involved and selling them on the idea. It was a very resource-intense investigation, as you can imagine.

But the premise of the investigation was different than it had ever been done before. Our idea was to follow the money, using that old phrase. But follow the money is very, very important. This is a multi-billion dollar worldwide industry. So the first thing we did was to approach MasterCard, Visa and American Express. Since almost all this Internet child pornography is processed through credit cards, we wanted to have real time access to the transactions that were occurring on these child pornography websites. After negotiation with MasterCard, Visa, and American Express, I think, for the first time they gave us that real time access. From there, we were able to trace it to what were in essence the money launderers here in the United States, a place called Connections USA, which operated out of the State of Florida. They were processing millions of dollars a month in transactions from these child pornography websites.

Once we were able to establish that they were getting illegal money from these websites, we approached them, were able to arrest them and then turn them to cooperate for us, and they, then, turned us to RegPay, which was their client in Belarus. This is where the child pornography was being created, this is where it was being put up onto the Internet websites. And there were principals that operated out of Belarus that were interacting on a regular basis with these folks in Florida. And as I said, the folks in Florida were laundering millions of dollars a month for these people through American banks, American credit card companies, back over to Belarus.

We were able to execute, with the help of these cooperating witnesses in the United States, a successful lure, and that is to lure these folks from Belarus to a place where we would be able to arrest and successfully extradite them to the United States. The lure occurred in Paris. We were able to tape record very incriminating conversations with these people from Belarus in Paris. Once all the incriminating conversations were taped by the cooperating witness, they were arrested, put in jail in Paris and extradited to the United States.

We have obtained guilty pleas from all the principals of the RegPay company in addition to the guilty pleas we got from Connections USA. Those people are about to be sentenced, Mr. Chairman, and they have presumptive sentences somewhere between 25 and 30 years. That, given the recent Supreme Court decision in Booker, the guidelines are no longer, as you know, mandatory but advisory, but we are confident that we will get very significant sentences and we will argue for 30-year sentences for these folks.

This case is significant, in essence, because following the money gets you to the people who are creating this child pornography, exploiting these children and putting these images up on the Internet and

we were also able to get those people in between who are profiting from the money laundering for these folks. So this is something that can be done; the template is out there now for other U.S. Attorneys' offices. We have worked with a lot of them in an attempt to show them how we did what we did. We are enormously proud of the efforts that started with that one assistant United States Attorney who had a different idea about how to go after this problem.

I thank you for the time.

[The prepared statement of Hon. Christopher J. Christie follows:]

PREPARED STATEMENT OF THE HON. CHRISTOPHER J. CHRISTIE, UNITED STATES ATTORNEY, DISTRICT OF NEW JERSEY, U.S. DEPARTMENT OF JUSTICE

Chairman Whitfield, Ranking Member Stupak, and distinguished members of the Subcommittee, thank you for inviting me to testify before you today about my office's prosecutions of cases involving the sexual exploitation of children on the Internet, including the RegPay case, in which we prosecuted both producers and consumers of child pornography.

Introduction

As this Subcommittee is already no doubt aware, the advent of the Internet has led to a vast proliferation in the availability and prevalence of child pornography in today's society. The possession and distribution of child pornography ware once relatively rare crimes relegated to those who would frequent certain underground adult bookstores or attempt to order obscure magazines from overseas. The Internet has dramatically changed that by making child pornography easy to produce and distribute, while also making it readily available to those inclined to seek out this material from their own home. Sadly, thousands of individuals who are sexually attracted to children now have ready access to images and videos depicting the sexual exploitation and molestation of children. Moreover, unscrupulous and opportunistic individuals both here and especially abroad have seized the opportunity to market access to child pornography in an industry that provides huge profits and relatively low overhead costs. It is probably accurate to say that the number of individuals in this county who have intentionally obtained access to or traded images of child pornography within the last six-month period outstrips the number for a similar six-month period from 15 years ago by at least a hundredfold. In addition, the Internet has also become an avenue for child predators to seek out and communicate with children in the seeming anonymity of chat rooms.

Needless to say, this sea change has created a tremendous challenge for law enforcement -- one that requires law enforcement to adapt quickly to a rapidly changing landscape and to search for innovative ways to identify and apprehend offenders. It has also put a premium on law enforcement officers with technological and computer expertise.

Law enforcement efforts to interdict Internet-based child exploitation crimes are largely dictated by the nature of the offense, which can be loosely grouped into two categories: child pornography offenses and child exploitation cases. The former type of investigation is more heavily dependent on technological expertise and forensic investigation, while the latter is typically dependent on the capacity of an individual agent to convincingly portray himself or herself as a minor who is susceptible to advances by on-line predators.

To understand child pornography offenses and the efforts of law enforcement to effectively investigate them, it is necessary to understand the nature of child pornography

on the Internet. Much of the proliferation of child pornography can be traced to the existence of numerous commercial websites that offer access to child pornography for a monthly fee. During the past ten years, hundreds of websites, many based in Eastern Europe, have appeared on the Internet. These sites typically require a subscriber to submit various information including billing information, whether it be via credit card or some other on-line payment service such as E-Gold. Law enforcement efforts to interdict these websites and to apprehend both those who operate them and those who subscribe to these sites has proven a formidable task, but there have been notable successes. Foremost among these successes has been the RegPay investigation which represented the collaboration of a number of federal agencies, including the Federal Bureau of Investigation (FBI), the Department of Homeland Security's Immigration and Customs Enforcement (ICE), the Internal Revenue Service Criminal Investigations, and the Postal Inspection Service, in conjunction with the United States Attorney's Office for the District of New Jersey and the Child Exploitation and Obscenity Section in the Department's Criminal Division (CEOS). It is also illustrative of how the federal government can successfully target the commercial child pornography industry at both the level of the producer and the consumer.

The RegPay Case

The RegPay investigation, which began in early 2003, represented the first large-scale effort to target the operators of commercial websites offering access to child pornography over the Internet and to track the financial trail created by those who profit from this industry. In the early part of that year, federal agents made undercover purchases of monthly subscriptions to numerous child pornography websites in an effort to track down the producers of the material and the operators of the sites. The investigation revealed that a company based in Belarus, which called itself RegPay, operated several commercial child pornography websites and processed credit card fees for more than 50 other similar sites. The investigation also determined that credit card payments for access to these sites were being processed through a company based in Ft. Lauderdale, Florida known as Connections, USA. Agents also executed search warrants on computer servers based in Texas and Virginia that RegPay had leased, and recovered extensive databases documenting credit card transactions involving approximately 90,000 customers worldwide. Armed with this informatio,n the investigation pursued two paths, aimed at, on the one hand, the operators of RegPay and those who processed their transactions, and, on the other hand, the consumers who purchased access to the site.

To pursue the operators of RegPay, agents first executed a search warrant at Connections, USA in Ft. Lauderdale. Upon executing the search warrant, agents learned of an ongoing financial dispute between Connections, USA and the operators of RegPay relating to an outstanding debt of more than one million dollars supposedly owed to RegPay. Agents were able to assume the role of Connections, USA to broker a meeting in Paris between the operators of RegPay and Connections, USA, ostensibly to resolve the ongoing dispute and to set the groundwork for future financial cooperation between the companies. This ruse led to the arrest of two Belarussians in Paris while a third individual was apprehended while vacationing in Spain at the same time. All three were extradited to New Jersey to face charges relating to the production and distribution of child pornography. All three pled guilty on the eve of trial in February of 2005 before the Honorable Dennis M. Cavanaugh of the United States District Court of New Jersey. The two principals of RegPay, Yahor Zalatarou and Aliaksandr Boika, are expected to be sentenced later this month. They face presumptive sentences in the range of 25 to 30 years. In total, 9 individuals pled guilty in the District of New Jersey for their involvement in operating or supporting RegPay's business operations, including three individuals from Connections, USA as well as three California-based individuals involved in the laundering of RegPay's proceeds. One of these latter individuals,

Yaroslav Grebenschikov, admitted that in late June 2003, he assisted individuals associated with Regpay in the formation of LB Systems - a company created to assist Regpay and others in Belarus to process credit card sales for previously approved transactions involving child pornography - as well as the opening of a bank account, both of which he used to transfer more than $200,000 in funds associated with RegPay to banks in Latvia.

Simultaneously, in what was dubbed Operation Falcon, agents pursued the consumers of child pornography by following the transaction history of those who had gained access to the RegPay-supported child pornography websites. By comparing the transaction data obtained via the search warrants conducted on the servers in Texas and Virginia with credit card records, agents were able to seek search warrants for numerous individuals throughout the United States. Leads were also distributed worldwide to pursue those who knowingly received and possessed child pornography. Through February of 2006, the RegPay investigation had resulted in 341 federal, state and local arrests in the United States and approximately 703 additional international arrests. In the District of New Jersey alone, more than 50 individuals were charged federally with possession of child pornography. The New Jersey defendants included teachers, a pediatrician, a psychologist, a retired minister and, perhaps least surprisingly, several individuals who had been convicted of sex offenses against minors, including a former school principal.

Recidivist Offenders

This latter category illustrates the importance of pursuing the consumers of child pornography because, among other reasons, the link between those who seek out child pornography and those who molest children is substantial and disturbing. Of the approximately 52 New Jersey targets charged federally in New Jersey, 5 had prior convictions for sexual offenses against minors. In addition, 3 other defendants, when confronted by ICE agents conducting searches on their computers, admitted to molesting a total of at least 14 children, while two defendants, including one of the convicted sex offenders, admitted to attempting to meet minors in on-line chat rooms. What cannot be known is how many others of those who were arrested had molested in the past but chose not to reveal this to authorities. While it is uncertain what percentage of those who gain access to child pornography act out upon their impulses, it is clear that a significant percentage do and common sense dictates that the exposure to child pornography encourages this behavior. For example, a study completed in 2000 by the Director of the Sex Offender Treatment Program at the Butner Federal Correctional Complex in North Carolina revealed that of 54 inmates convicted of child pornography offenses, 79.6% of them admitted that they had also molested significant numbers of children.

Harm to Exploited Children

Furthermore, the proliferation of child pornography websites and the great profits reaped by their operators fuels a market for the production of new and often hard-core child pornography. In short, the market in child pornography directly leads to the exploitation and molestation of children from all over the globe, often for the purpose of commercial gain. Many of the victims are from Eastern Europe where a substantial percentage of child pornography is produced. Images and videos of American children are encountered with great frequency, however, because once a photograph of child pornography makes its way on to the Internet - something that can be accomplished with ease in the era of digital photography - control of that image is essentially lost, and commercial websites may include such images in the collections they offer on their sites. Sadly, the victimization of children forced to become the subjects of child pornography thus continues as the image travels throughout the Internet. As Attorney General Gonzales noted recently, "[child pornography] is not a victimless crime. Most images

today of child pornography depict actual sexual abuse of children. Each image literally documents a crime scene."

The Evolving Landscape and Law Enforcement's Challenge

As with most sophisticated criminal enterprises, the purveyors of child pornography adapt to law enforcement techniques, thus forcing investigators to adjust to an ever-changing landscape. The commercial child pornography industry has evolved even since the RegPay investigation. For instance, child pornography websites are not as easily located on the Internet by the uninitiated as was the case three to four years ago. While this may reduce the number of individuals subscribing to these sites, it also makes them harder for law enforcement to locate and identify. Moreover, the operators of these sites are increasingly sophisticated in hiding their own identities and whereabouts. They accomplish this both technologically - by making their operations more difficult to trace through the use of such software as anonymizers - and by insulating themselves through the use of sham Internet-based companies and other third parties through which they funnel their profits from the child pornography websites. Moreover, they lease server space typically through the use of stolen identities, and the companies that lease the space to them frequently do not realize the true content of the website they are helping to host. Perhaps the greatest challenge to bringing these individuals to justice, however, stems from the concentration of such operations in Eastern Europe, typically in the break-away Soviet republics such as Belarus. Most of these countries do not have extradition policies with the United States, and the knowledge of the fate of the RegPay defendants makes the likelihood that operators of similar sites will venture outside the relative safety provided by the borders of their home country remote at best. Widespread corruption amongst Government officials in some of these countries significantly reduces the chances that they will face meaningful prosecution in their homeland.

These obstacles mean that curbing demand for child pornography will be increasingly important in combating the proliferation of this material. Techniques including electronic surveillance and the execution of search warrants on servers both domestically and abroad provide a deterrence effect for those who might seek child pornography through online commercial websites. Law enforcement needs to send a clear message that individuals who subscribe to these websites and contribute to the molestation of children across the globe run a substantial risk of facing significant jail time any time they hit the "JOIN NOW" button for one of these sites. As I speak here today, even though child pornography websites are harder to locate than before, there are still thousands of Americans who attempt to subscribe to child pornography websites every month. Law enforcement can and will play a significant role in bringing such individuals to justice.

Alternative Distribution Methods

While I have spoken so far primarily about the role of commercial websites in the proliferation of child pornography, it is important to realize that a great deal of child pornography gets distributed on the Internet through individuals who trade such material with one another. Additionally, peer-to-peer software such as Kazaa and Limewire may be abused by those with a mutual interest in child pornography to share their respective collections with one another if they belong to the same network of computers. Child pornography may also be distributed through attachments to e-mail. Individuals with an interest in child pornography may frequent certain chat rooms from which they will exchange collections. In addition, certain individuals may establish on their home computer what is known as an F-Serve on which they establish a collection of child pornography that can only be accessed by those who upload images of child pornography to the F-Serve first - thereby preventing law enforcement from gaining access while expanding the F-Serve operator's own collection.

All of these methods for distributing child pornography cause many of the same harms as posed by commercial child pornography websites, namely, the continued victimization of the children depicted and the encouragement of those with pedophilic impulses to act upon them. Law enforcement can identify many of the individuals involved in these forms of distribution through a variety of techniques. For instance, certain programs can be run which search computers that are connected through the same network for a particular image as defined by its hash value. This enables law enforcement to identify individuals who have particular images of child pornography on their computers and may establish sufficient probable cause for search warrants. In addition, forensic examination of an individual's computer that has been seized may reveal e-mail communications with other individuals who have sent and received child pornography from the seized computer. In this regard, traditional cooperation from a defendant who has distributed child pornography through these means may lead to the identification and arrest of numerous others.

Interstate Traveler Cases

In addition to investigations involving child pornography, the FBI plays a vital role in preventing and even interdicting child exploitation crimes so long as there is some interstate nexus to provide federal jurisdiction. The best known example of this type of investigation is the so-called enticement or "traveler case," which has been recently well documented on a series of "Dateline NBC" episodes. Across the country, too many of our children have been lured by child abusers through contacts in chat rooms that are allegedly closed to adults. Some of these interstate travelers also take pictures of the minors they molest and sometimes abduct, and then post the child pornography online. This type of investigation requires an undercover agent to enter an Internet chat room where older men are likely to be interacting with minors. The undercover agent will engage in a series of chats to determine if the other individual is an adult seeking sexual contact with the undercover whom he believes to be a young teenager. As the chats progress, the older male may decide to travel to the location of the minor in the hopes of renting a nearby motel room or making similar arrangements. If the older male travels across state lines to meet the minor, the case may be taken federally. While many "traveler cases" may be prosecuted at the state level, federal traveler cases are not uncommon. For instance, the District of New Jersey is currently prosecuting a case where a doctor from a prominent Philadelphia hospital traveled to Hackensack, New Jersey expecting to meet a 14-year old girl with whom he intended to have sexual relations. Such "traveler cases" often involve actual minors whom the traveler intends to sexually abuse. For example, the District of New Jersey recently secured a conviction of a Florida man who traveled to New Jersey to have sex with a 13-year old girl. ICE agents, who did not initially know the identity of the intended victim, trailed the defendant and observed him following a school bus in an effort to find the girl whom he had met over the Internet. The agents were able to interdict this crime before the defendant, who was in possession of a stun gun and alcohol, contacted the victim. It is likely that such crimes, however, are greatly under reported by the young and confused victims.

Sex Tourism Cases

Another, albeit less common type of child exploitation case that may involve the Internet arises out of sex tourism investigations wherein the defendants are individuals who travel overseas to have sex with minors, or who organize such trips. These trips frequently involve travel to southeast Asia. Sex tour operators catering to pedophiles tend to be discreet and are difficult to infiltrate because they are usually extremely wary of law enforcement. If successful, however, these cases may not only lead to the apprehension of the tour operator, but his prior clients as well. Because of the

international nexus of these violations, ICE often acts as the primary federal law enforcement agency responsible for conducting such investigations. ICE has conducted many successful child sex tourism investigations and works closely with CEOS, the U.S. Attorney's Offices, as well as federal, state and local law enforcement agencies.

The District of New Jersey is currently prosecuting one such case where the defendant operated a website advertising sex tourism. The website did not specifically advertise that its tours were catered toward minors, but it included pictures of girls in various states of undress, some of whom clearly appeared to be underage. The investigation involved undercover Internet chats followed by meets wherein undercover agents posed as customers seeking to have sex with underage girls upon arrival in the Philippines. The defendant initially indicated that he would not talk about minors until the group arrived in the Philippines, but he gradually opened up to the point where he admitted to having sex with minors himself.

Project Safe Childhood

All of the investigations that I have described so far will be bolstered by the Department of Justice's recently launched Project Safe Childhood initiative designed to coordinate the efforts of federal agencies and U.S. Attorneys' Offices with state and local law enforcement. This initiative is designed to help coordinate national child pornography investigations, train additional federal, state and local law enforcement in pursuing computer-based investigations and raise community awareness of the dangers of the Internet for children. The initiative is also designed to increase federal involvement in many of these investigations, especially where state laws provide little deterrence for offenders. This latter point is clearly evident in New Jersey where possession of child pornography regularly results in sentences of 2 to 3 years if prosecuted federally but carries with it a presumption of a probationary sentence under state law.

I am proud that the District of New Jersey has been a leader in pursuing child exploitation offenses on a national level, as evidenced by the RegPay case, which represents one of the most successful child pornography investigations in the nation's history. Most importantly, Project Safe Childhood will ensure that every state and every district has properly trained law enforcement officials who can vigorously pursue predators and similar offenders, when supplied with appropriate leads, and that these investigations will realize even greater success in the future.

I should also note that the District of New Jersey's experience in pursuing RegPay and other similar investigations demonstrates that the number of child pornography and other child exploitation offenders is quite simply staggering, and that it behooves law enforcement offices - whether they be the prosecuting authority or the investigative agency - to devote greater resources and personnel to these investigations. The RegPay investigation demonstrates that a few well-trained and dedicated law enforcement officials can make a major impact and provide prosecutors and agents in their own and other districts with large numbers of dangerous offenders to pursue and bring to justice. Unfortunately, sometimes our own American youth are the victims of traffickers in this country who lure youth from their communities and sell them for prostitution in other jurisdictions, offering them for sex at truck stops, conventions, and on the streets of our cities.

Human Trafficking

I would be remiss if I did not mention that the impact of federal law enforcement's efforts to protect children is not limited to investigations focused on the Internet. One type of crime that frequently entails the exploitation of minors are those involving human trafficking, whether they involve forced labor or sex trafficking. Many of the victims of this type of deplorable crime are minors, and they are often sexually exploited on a commercial basis. Human trafficking is a crime that has been with us for many years, but

continued largely unnoticed until the passage of the Trafficking Victims Protection Act of 2000, authored by a strong, committed group of legislators including Representative Christopher Smith, from my home state of New Jersey. That legislation recognized that many individuals, typically young female immigrants, were being smuggled into the United States and forced to work in demeaning conditions or in prostitution. Since the passage of that legislation, numerous trafficking cases have been brought throughout the United States, and the District of New Jersey has once again been one of the leaders in pursuing these types of cases.

In 2002, for example, this Office brought the case of *United States. v. Jimenez-Calderon* which led to the convictions of two women for their role in forcing several juvenile Mexican girls to work as prostitutes in Plainfield, New Jersey. The defendants received sentences of approximately 17½ years each. In 2005, this office indicted the case of *United States. v. Luisa Medrano, et al.,* which involved the smuggling into the United States of young Honduran females, some as young as fourteen, after they had been promised legitimate waitressing jobs to lure them into the country. Upon arrival in Union City, New Jersey, these girls were forced to work six or seven days per week at bars catering to male immigrants where they were pressured to perform sexually provocative dances for the customers and ply them with alcohol. The victims were also required to live at specific residences and had their movement greatly restricted until their smuggling debts were paid off in full. Many of these juveniles were sexually exploited during the smuggling process that brought them to New Jersey.

Even more recently, the District of New Jersey has brought various charges against a number of defendants for their involvement in prostitution activities in Hudson County and elsewhere. These defendants are primarily members of the Notario family from San Miguel Tenancingo, the trafficking capital of Mexico. The investigation has identified numerous trafficking victims who were put to work as prostitutes in various brothels along the East Coast after having been smuggled in from Mexico. Among these identified victims are at least three juveniles. Thus, the pursuit of human trafficking cases often represent yet another means by which law enforcement identifies and dramatically assists sexually exploited minors.

Conclusion

In conclusion, the dangers of the Internet in the proliferation of child exploitation crimes cannot be underestimated. The Attorney General has recognized that "we are in the midst of an epidemic in the production and trafficking of movies and images depicting the sexual abuse of children," and the need for law enforcement to respond rapidly and forcefully cannot be more clear. With proper coordination and the cooperation of federal, state and local authorities, the Internet can be made far safer for the children of this country. Law enforcement must create an environment in which sexual predators fear the Internet as a dangerous place that may likely land them in prison for a significant period of time. The RegPay investigation - especially with the advent of Project Safe Childhood - provides a model for law enforcement agencies throughout the country to pursue child exploitation cases with the knowledge that the offenders who are identified will be vigorously investigated and prosecuted.

Mr. Chairman, I again thank you and the Subcommittee for the opportunity to speak to you today, and I would be pleased to answer any questions the Subcommittee might have.

MR. WHITFIELD. Well, Mr. Christie, thank you very much and we certainly appreciate the great work you are doing here and I know there has been national attention on the prosecution in the RegPay case and I mentioned this in my opening statement, that those of us on the

committee have really been shocked about exactly how widespread this problem of child pornography is and then those people whose sole goal is to meet young people and meet them physically and molest them in some way. I know we had this case in Texas where a couple, a married couple, had a 5-year-old child and they had 7,000 subscribers, 70,000 subscribers that were paying $30 a month and they would molest their child sexually on demand and their income was around $2 million a month and through law enforcement and the techniques that you are using, that couple was arrested, prosecuted and both of them are now in prison serving between 40 and 50 years in a penitentiary.

But once again, I do want to commend you on the RegPay case and I would like you to elaborate, if you wouldn't mind, just a little bit about, in some cases and some jurisdictions, there is a lack of cooperation between Federal and State and local officials: Do you feel comfortable that on this issue that you are getting cooperation at all levels?

MR. CHRISTIE. As I said, Mr. Chairman, in my remarks, I think in this jurisdiction I can speak to this one with the most knowledge. There is a great deal of cooperation. I think part of that is led by the fact that there is so much of this crime going on, that there is so much to go around, that people aren't arguing over who gets what case. It is more trying to figure out how do we cover everything we need to cover. The breadth of the problem is extraordinary. As I said, it is a multibillion dollar industry and it branches off in a number of different directions.

You have the exploitation of the children, as you mentioned, who are in the images. And in our office, we have had cases with children as young as 6 months old who are being exploited sexually on these images, which I will tell you, I was not in law enforcement before I became the United States Attorney, and when I saw these images of children as young as 6 months old being exploited, it is the most sickening thing I have seen in this job, so I think the cooperation is driven by the depravity of the crime and also by, unfortunately, the volume of it. We all need to work together and there is plenty for all of us to do.

MR. WHITFIELD. Right. Now, what about Attorney General Gonzalez's Project Safe Childhood initiative? What is your view on that and are you pleased with that?

MR. CHRISTIE. I think it is a very important initiative, but one in New Jersey that, quite frankly, we were ahead of. When you look at what Project Safe Childhood is asking U.S. Attorneys offices to do, is ordering the U.S. Attorneys offices to do, we have already done that 4 years ago. When I became U.S. Attorney, we set up a separate stand-alone unit on that which was called our Public Protection Unit that deals almost exclusively with crimes against children. We have seven assistant United States Attorneys who are working almost exclusively on

that, also with violence against women and human trafficking, so the initiatives that the Attorney General is calling for in terms of the focus there, is something that we have been doing for the last 4 years. In fact, the chief of my Public Protection Unit is here with me today, Mark McCarren, and Mark has been working on these problems with me now for nearly the last 4 years, so I think the focus is very important.

In addition, I think it helps to focus the other investigative agencies, both inside DOJ and outside the Department on making sure they make these investigations a priority, so I mentioned in my remarks they are very resource intensive. You will have hundreds and hundreds of targets that you need to go after across the country and sometimes around the world, so you need the cooperation of the FBI, you need the cooperation of Immigration and Customs Enforcement out of Homeland Security to make sure that they put the resources on it. So I think the Attorney General putting a focus on it will help to make sure those other resources come, as well.

MR. WHITFIELD. What was the length of time from the beginning of the RegPay case until you did get a conviction?

MR. CHRISTIE. It was about 2 years.

MR. WHITFIELD. Two years?

MR. CHRISTIE. About 2 years.

MR. WHITFIELD. You know, we also had, in one of our hearings, there was a young girl from Russia who was adopted by a gentleman here in Pennsylvania. She was 6 years old, and it came through a child adoption agency in New Jersey and this child was placed with this man who was not married and for a period of 6 years he sexually molested her, kept her chained in the basement for periods of time, taking obscene pictures, and putting it all over the Internet, which he was paid for that, as well. And through some very innovative work by law enforcement, he was also arrested and is serving a prison term now. We are going to have a hearing about some of these child adoption agencies, in which this agency received a fee of $25,000 and did not do any due diligence in placing this child. It also appears, we are going to be looking into that aspect, which is a little bit different than we normally think, in these cases.

At this time, I would like to recognize Mr. Ferguson for any questions he may have.

MR. CHRISTIE. Mr. Chairman, I need to say just one thing before Mr. Ferguson, on that point; there are many branches of this problem and you have just raised one of them and human trafficking is also a part of this problem. You can identify these people as people who exploit children sexually from a child pornography perspective, but also, a lot of these organizations are involved, especially in Eastern Europe and in

Central America, in highly coordinated trafficking of individuals into the United States for children for this very purpose. And so I would urge the committee, as they go forward, to not lose sight of that aspect of this, as well, because the profits being made there are not as significant as in the pure child pornography industry, but they are significant and it is a growing problem here, especially in a State like New Jersey, where you have a real melting pot and so people can come from very different parts of the world and fit in here seamlessly and not be noticed.

MR. FERGUSON. Thanks, Mr. Chairman. Thank you again for being here with us today, Mr. Christie. We have had a number of these hearings. We have heard from lots of different folks, including victims. You talked about the volume as being a challenge, an issue that you have to deal with. One of the victims that we heard from in one of our first hearings who actually turned this into a business for himself when he was, himself, a minor; ended up making a lot of money.

He finally decided to turn over all of his information to legal authorities and he testified that he was--this is another part of the country--was very, very dissatisfied, disappointed with the pace of the law enforcement investigation. To his knowledge, this is some months or a couple of years, I think, after he had turned all this information over to the Department of Justice, that they hadn't, as far as we know, hadn't brought a prosecution or hadn't had a conviction of, I don't know, some 1,500, I think, IP addresses and credit card information and there clearly are a lot of challenges for law enforcement, for folks like yourself, to try and get to the root of this problem and to prosecute and hold accountable those who need to be held accountable.

We are trying to address that from a legislation point of view, if that is necessary. What insights can you share with us? What challenges, what problems do you see, from a Federal law enforcement perspective? What challenges do you have in terms of trying to go after these folks? You have obviously had success, so you have overcome some challenges, but what other, what insights can you share with us? What can we be doing from our end to help work with law enforcement, particularly Federal law enforcement?

MR. CHRISTIE. Well, we have had--I don't want to lead anybody astray. We have had our frustrations, too, and they surround, essentially, resource-type of frustrations where you really need to get people focused. This work is difficult work and quite frankly, Congressman, it is distasteful work. When you have assistant United States Attorneys and agents who are working day after day amidst these images, at times it can be inspirational because you want to try to save these children, but it can be very emotionally taxing and so part of what we have done is try

to rotate the people that we have doing this work to try to ease the burden from them because it is an extraordinary burden.

If you sit and leaf through, as I have, notebooks of these images, it is extraordinarily disturbing. And as a parent, you can't but have your mind wander to how horrible the reality is for these children. I think in terms of what can be done, I think the Attorney General's step is a good one. I think we need to just make sure that law enforcement understands that this is a priority, that this is important work that we need to do, and that is about providing leadership and that is why I think the Attorney General's initiative in Project Safe Childhood is so important.

We saw, in the first term of the Bush Administration, the focus on Project Safe Neighborhood and on violent crime and we had enormous results from that initiative. I think we can have similar type of results in this initiative just by the Attorney General telling every U.S. Attorney this now must be a priority in your office. In some offices, like mine, it already has been, but in others it hasn't and so in those offices they now know, from the number one guy in our department, that this is a priority and I think anything that Congress can do to encourage and supplement that leadership is going to be very important because they need to know from the Congress that they think this is important, as well.

MR. FERGUSON. You talked about, sort of, this fatigue that can set in when dealing with a topic which is so distasteful and so horrible. I spent a day over at the National Center for Missing and Exploited Children, meeting with the folks there who are doing this every day. They do lots of things there; as you know, they train law enforcement from all around the country, they bring them in for free and train folks, which is an incredible service, but they also have this Federal kind of a task force with all different folks from FBI and DOJ and all different folks trying to work together and one of the things they do is monitor all of this material and try and get their hands on this material and figure where it came from, who created it and whatnot. And it has got to be a tremendous strain and a mental and psychological strain for just a human being; these are just people that are doing this investigative work. So that sort of having to rotate folks through opportunities like that has got to be very difficult because, I mean, just thinking about it from our perspective and listening to testimony, it is horrible.

MR. CHRISTIE. Yes.

MR. FERGUSON. And for folks who are doing this every day, it must be really, really difficult.

MR. CHRISTIE. It is, and I think one of the things that have escalated that, too, through the Internet in particular, is not only the availability of it in everybody's home now, but the fact that there are really two ways to pay for this material that are being used now. It is not only just paying

through credit card, but you can pay by uploading your own images. So you can pay in kind, essentially, so that if you are willing to upload 30, 60, 90, 120, they usually do it in lots of 30, original images of child pornography, that can help to pay for your membership to these type of sites, instead of paying cash.

We have had cases where you have people who are exploiting their own children in order to have access to this information, in order to make a profit. You have people out there, we have had cases of people adopting children, as you mentioned, and not just foreign adoptions, but domestic adoptions, where they then trade their children with other pedophiles and allow them to abuse their children in return for abusing someone else's children.

The breadth of these crimes and what I am really trying to get across is, the focus on the Internet is important because of its availability and its ability to exploit our children in our own living rooms. But we need to make sure that we follow all the branches of what runs off of this vein and it is an enormous problem and one that we are spending a lot of time, you know, seven--I have 130 AUSAs in my office, seven of them are working just exclusively on this type of work, so that is a large commitment of resources, from a percentage perspective, on crimes against children and we include human trafficking in that, as well, since most of the people trafficked are children, so it is a fatigue area and so I try to move my people out of there, except for Mark, who is, unfortunately, stuck there because he does it so well. But he has shown real leadership in that area and he has gotten a lot of new young people in there now that we have just put in that are really bringing an enormous energy to the task.

MR. FERGUSON. I happen to know Mark. He and I went to high school together many moons ago and you are fortunate, as you know, to have such a talented person leading the charge on that.

MR. CHRISTIE. Absolutely.

MR. FERGUSON. Mr. Chairman, I have one more topic I would like to cover with the U.S. Attorney.

MR. WHITFIELD. Sure.

MR. FERGUSON. You talked about following the money. You talked about how this is paid for, largely through credit card companies and using that technology. How can we work with, in your opinion, with your experience, how can we work with the credit card companies to make them a full partner in this effort? It just seems to me, and this is another thing that has become obvious to us in other hearings, is that without the money, a lot of this problem, not all of it, but a lot of this problem is driven by money and by the ability for people to make money and the commerce of the issue is really, I think, perhaps at the heart of

this, other than just a sickness. How did you work with the credit card companies in the RegPay case and how might that be a model and what things have we learned from that? Or what things do we need to do to help them to be a more active partner with us in this effort, as well? Because I have got to believe they have got to be a huge part of it.

MR. CHRISTIE. Well, they are an enormous part of it and this former AUSA identified that very early on and was his first foray into trying to set this up was meeting with the credit card companies. And I will be candid that initially we met with some resistance from them in terms of them giving us real time access to the transactions coming off these sites, but eventually, we were able to persuade them that this was in their interest.

And I think that anything that Congress can do to encourage both transparency on this topic from the credit card companies and real time access for law enforcement to these records, because listen, we know that if they are processing transactions from a child pornography website, that is illegal. So you have already met the threshold. This is not a free speech question. It is not a privacy question. These are people who we know are engaged in illegal conduct and they are using those credit cards to engage in that illegal conduct.

So I think to the extent that Congress can continue to prod the credit card companies to have transparency on this issue and give real time access, because the hundreds of thousands of transactions that are done, just in New Jersey every day on these websites, it is staggering. When you go across the country, you are talking about millions. So for law enforcement to follow those transactions, both to the people who are purchasing and then back to the people who are benefiting from this money, we need to get on top of it right away. People change credit cards, drop credit cards the same way that drug dealers change and drop cell phones, so we need to be on top of that and get that in a real time way because the money launderers here in the United States are also profiting from this, these middlemen companies who don't have any direct--they are not owned by the credit card companies, but they work as affiliates who are processing this money.

They are the key, after the credit card companies. Once you get to them, they know who they are making these deals with around the world and how much they are getting paid to process this money and get it to foreign banks where we would have a more difficult time seizing the assets. So I think the credit card companies are the gateway into this industry and so to the extent they can continue to be held accountable for transparency and giving us real time access, the Congress would be making an enormous contribution in that regard for law enforcement, to make our job easier and make us more effective.

And I will tell you, these guys in the RegPay case were stunned that we were able to catch them, we found in debriefings afterwards, because no one had ever followed the money before. The traditional way law enforcement had done this was to just go after the purchasers. It is the easier way to go. And a lot of time it is important, because in this case, we had purchasers who were pediatricians, purchasers who were school bus drivers, purchasers who were athletic coaches for children.

You need to go after those people to get them out of circulation because the statistic, Congressman, you mentioned, about how apt these people are to be able to then act out on the abuse is they own this material. So both sides are important, but there had been an emphasis in law enforcement previously just on the purchaser side and not on the side of the people who are profiting from this monetarily.

MR. FERGUSON. Actually, I have another question. Do you mind?

MR. WHITFIELD. No, go ahead.

MR. FERGUSON. I have one more question. When it comes to ISPs, we have also been in conversations and heard testimony from ISPs, these Internet Service Providers who--there is no real industry standard right now for the length of time that they keep information and we have heard from law enforcement, the Department of Justice, and others who would like there to be a standard where ISPs would keep information about traffic and personal information from folks for up to 2 years. ISPs and other privacy organizations, frankly, have raised concerns with that. Do you have any particular personal or professional recommendation on where we--I mean, ideally we will come to some consensus on this and bring everybody together, but in the case that we may end up having to legislate this at some point, do you have any insights for us on how that might affect your ability to go after the bad guys?

MR. CHRISTIE. Well, without talking specifically about legislation, it seems to me that from a law enforcement perspective, having that historical information is the only way that we are going to be able to follow these people unless you are in a situation where you are real time following it in the midst of an investigation. If you want to try to do one of these things historically, which is most of the time the way it is going to be done, the RegPay case is an anomaly. Most of the time you are going to wind up kind of backing into one of these investigations and so having that historical information available to us is important, and I understand the privacy concerns of gathering and holding onto--for the ISPs, holding onto this personal information.

But again, it seems to me that law enforcement, in this instance, is only going after folks and only requesting information on folks who are on child pornography websites. Per se, that is illegal. I mean, we are not talking about people who are going on adult pornography websites,

which you may or may not necessarily be illegal. We are not talking about obscenity in the adult obscenity sense, which some people may argue have some First Amendment protection. We are talking about children who are being exploited sexually for profit on the Internet. There can't be any argument from anyone that there is a privacy protection, in my view, here. What is the privacy protection of people profiting illegally from exploiting children, both in the United States and around the world.

And so I have less sympathy for the privacy position in this particular context, because the underlying conduct is, per se, illegal. And once you have established that, it seems to me that if we establish probable cause to get the information and have a judge who is willing, a Federal judge, lifetime tenure, who is willing to sign off on a search warrant for us to be able to get those materials, it seems to me that the privacy issue is much less important and so I would be hopeful that Congress can help in forging a consensus among all the parties on this, but if not, I think it is a very important tool if we are really serious about going after these folks because I will tell you, they believe--when they sit in their living rooms--we have spoken to people who are purchasers of this material. When they sit in their living rooms, they believe they are anonymous. They believe no one knows who they are and they don't grasp the fact yet that law enforcement can come and get them for doing this and that they are part of the problem. And I think we need to send very strong messages about that and that is why, in our office, we have been as aggressive as we have been, not only on the RegPay supplier side, but on the purchaser side, as well. And it is important that if Congress sends that type of message, I think the Federal judges will hear it, too, and will make sure that in this era where they now have a lot more discretion, will give out stiff sentences to these folks, because these are serious crimes.

MR. WHITFIELD. I think Congressman Ferguson did hit on an important part and that is relating to data retention and we have had a number of meetings with the Internet service providers and maybe not surprisingly, they haven't talked a lot about privacy with us; they talk about cost with us. But we have told them that we think it is essential that they start retaining this data and I think the Chairman of our full committee and with Mr. Ferguson's help and others, are probably going to come forward with legislation to deal with this in a broader sense, as well. I am also glad you mentioned the credit card things because, as I mentioned in my opening statement, this is our fifth hearing on this subject matter and we are going to have another one and we are bringing in the credit card companies to see what we can do with them to assist in a more effective way, also.

MR. CHRISTIE. I will say it is really important, Mr. Chairman, and I have to give MasterCard, Visa, and American Express credit on the RegPay case. After negotiations with them, that were good faith negotiations, they came forward and gave us the access and the information we needed to make that case, so it is available and they can do it if they want to do it, and in the RegPay case, they did it and they were enormous partners in bringing that case to a conclusion.

MR. WHITFIELD. And I know Congressman Ferguson had also mentioned this young man who first got involved in this because an older gentleman convinced him that if he would take off his shirt with a webcam showing and everything, that he would send him a check for $50, so that was his first step down the road to being sexually exploited in person--by taking off his shirt and getting a check for $50. But thank you very much for your testimony and great leadership you are providing here in this area and we look forward to working with you as we continue down the road to take steps to reduce the exploitation of children on the Internet.

MR. CHRISTIE. Thank you. Thank you for inviting me, thank you for being here. I thank you for your focus on this problem. It is an enormous problem that really, quite frankly, when I go around our State, frightens more parents than almost anything because they really feel as if they have lost a sense of control over their children and so your committee's focus, subcommittee's focus on this is really important and I think gratifying.

MR. WHITFIELD. And so many parents are way behind their children about the way the Internet operates, too, which makes it more difficult.

MR. CHRISTIE. I count myself among them, absolutely. Thank you. Thank you, Congressman.

MR. WHITFIELD. At this time, I would like to call our second witness, and that is Congressman Michael Fitzpatrick, who represents the Eight Congressional District in Pennsylvania. Congressman Fitzpatrick, it is great to see you here today. As I mentioned, before you came in, Congressman Fitzpatrick, you have introduced a bill, H.R. 5319, entitled "The Deleting Online Predators Act," and I know you have been at the forefront on trying to deal with this issue, so we are quite excited about your being here today to testify. As you probably know, in Oversight and Investigations, we do like to take testimony under oath and I am assuming you have no difficulty in testifying under oath.

MR. FITZPATRICK. Sure.

MR. WHITFIELD. So if you would stand up and let me just swear you in, raise your right hand.

[Witness sworn.]

MR. WHITFIELD. Thank you very much and you are recognized now for 5 minutes, Congressman Fitzpatrick.

STATEMENT OF HON. MICHAEL FITZPATRICK, MEMBER, U.S. HOUSE OF REPRESENTATIVES

MR. FITZPATRICK. Mr. Chairman, Congressman Ferguson, thank you for permitting me to participate in your Oversight hearing this morning, allowing me to give testimony on what I feel is a new and emerging problem confronting our Nation's children and their safety while using the Internet. Mr. Christie correctly testified, indicated that this is a, virtually a multibillion dollar industry where the sole product is the exploitation of our Nation's children. And Chairman, you talked about the particular case, international adoption of a young girl, I believe she was from Russia, passed through an adoption agency here in New Jersey and ended up ultimately adopted by a single male in the western part of my State, I think it was Pittsburgh or Plum, Pennsylvania. His name is Mancuso.

And I remember her story, her name is Masha, and while she has been placed now with a real family, her innocent images, which were essentially stolen from her, continue widely available on the World Wide Web, and while Mr. Mancuso is in jail, there is legislation that has been introduced in the Senate, hopefully it will be introduced into the House soon that will give Masha private right of action against those Internet service providers and the providers of Internet e-mails who continue to profit from her innocence in her images, as I said, both were stolen from her, so I look forward to the introduction of that legislation, as well.

I want to thank the Subcommittee on Oversight and Investigations, Chairman Whitfield and Congressman Ferguson, for holding this, the committee's--I think you said it is the fifth hearing in addressing the dangers that online predators pose to our Nation's children. Your work in this area is helping to shed light on the difficult challenges to both law enforcement and to American families, as well, and I appreciate the committee's dedication to this issue.

As the father of six children, I know the challenges that technology poses to our families. In a world that moves at a dizzying pace, being a father gets harder all the time. Monitoring our children's use of emerging technology is a huge task and the Internet remains the focus of many parents' concerns. The technological breakthrough of the World Wide Web has been enormously beneficial to our society. The Internet has brought communities across the globe closer together through instant communication. It has enabled an unfiltered free flow of thought, ideas,

and opinion. The Internet has opened a window to the world right at our fingertips.

However, this window opens both ways. The freedom to connect to the world anywhere, at any time brings with it the threat of unscrupulous predators and criminals who mask their activities with the anonymity the Internet provides to its users. And among its many applications, one of the most worrying developments of late has been the growth of what are known as social networking sites. Social networking sites like Myspace.com is one of the more famous--Friendster and Facebook are some of the others--have literally exploded in popularity in just a few short years. MySpace alone has just over 80 million users and ranks as the sixth most popular English language website and the eighth most popular in the world.

Anyone can use these sites. Companies and colleges, teachers and students, young and old all make use of social networking sites to connect with people electronically, to share pictures, information, course work, and common interests. These sites have torn down the geographical divide that once prevented long distance social relationships from forming, allowing instant communication and connections to take place and a virtual second life to take hold for its users. For adults, these sites have been fairly benign. For children, they open the door to many dangers, including online bullying and exposure to child predators that have turned the Internet into their own virtual hunting ground.

I became personally aware of the danger of the Internet and what it can pose after my 16-year-old daughter began using the social networking site in MySpace.com. I quickly realized that while my daughter thought she was only chatting with her friends, other people, some with criminal intent, could be looking in. Although age limits exist on many of these sites, there is almost no enforcement of these rules. Frequently, children under the age of 14, which is the cutoff age for profiles on MySpace, simply lie about their age and fake being 16 or 18 or even older. Predators also use this anonymity to their advantage by profiling themselves as teenagers to more easily identify and navigate the profiles of their prey.

The dangers our children are exposed to by these sites is clear and is compelling. According to a study conducted by the National Center for Missing and Exploited Children, in 1998 there were 3,267 tips regarding child pornography. Since then, the number has risen by over 3,000 percent to an astounding 106,119 tips in 2004. The Department of Justice recognizes child pornography as a precursor for pedophiles and is often linked to online predators. According to Attorney General

Gonzalez, one in five children has been approached sexually on the Internet, one in five children.

Worse still, a survey conducted by the Crimes Against Children Research Center found that less than one in four children told their parents about the sexual solicitation that they received. MySpace, which is self-regulated, has removed an estimated 200,000 objectionable profiles since it began to operate in 2003. And while it is difficult to predict the exact number of total predators on the Internet at any one time, the FBI estimates that there are more than 2,400 active sexual, child sexual exploitation investigations under investigation at any one given time.

This problem is finally gaining the public's attention. Look closely at local and national news stories and you will undoubtedly see a story of a crime linked to a social networking site. Recently, national news reports have focused on the case of Katherine R. Lester, a 16-year-old Michigan honor student who fled to Israel with hopes of meeting a 25-year-old man she met on MySpace. Two months ago, in my own congressional district, right across the Delaware River in Bucks County, a 25-year-old man, Shawn Little, was arrested for posing as a teenager online to solicit a 14-year-old boy. Little's communications with the child resulted in a sexual encounter. And NBC's Dateline program has brought the threat of online predators to the televisions of millions of Americans through their acclaimed by disturbing "To Catch a Predator" series. While these high-profile cases make a splash in the headlines, how many other less-publicized cases of child exploitation go unnoticed?

While these stories have pressured many social networking sites to take action to improve their safety protocols, like MySpace recently has done, these changes, in my view, fall short of real reform and that is why I did introduce the bill, the Deleting Online Predators Act. Parents have the ability to screen their children's Internet access at home, but this protection ends when their child leaves for school or the library. My legislation would require schools and libraries in New Jersey and throughout our Nation to monitor the Internet activities of minors and implement technology to protect their children from accessing, number one, social networking sites like MySpace.com and chat rooms which allow children to be preyed upon by individuals that seek to do our children harm and also protect them from visual depictions that are obscene.

Preventing access to social networking sites in these situations is not designed to underestimate the importance of parental supervision. Internet safety begins at home and that is why my legislation would require the FTC to design and publish a unique website to serve as a clearinghouse and resource for parents, teachers, and children for

information on the dangers of surfing the Internet. The website would include detailed information about commercial networking sites. The FTC would also be responsible for issuing consumer alerts to parents, teachers, school officials, and others regarding the potential dangers of Internet child predators and their ability to contact children through MySpace.com and other sites.

In addition, the bill would require the FCC to establish an advisory board to review and report commercial sites and chat rooms that have been shown to allow sexual predators easy access to personal information of and contact with children. Make no mistake, child predators are on the Internet and they are a growing problem. Predators will look for any way to talk to children online, whether through sites like MySpace, instant messaging, or even online games. The best defense against these people is to educate parents and children of the dangers that come along with the Internet and by limiting access to certain sites during the school day.

And this is not all. Congress and State legislatures must also act to dedicate funds to law enforcement programs designed to combat child predators. Last month we fought for and in Congress we passed legislation to increase funding to the FBI's Internet Crimes Against Children Task Force and the Innocent Images National Initiative, which serves as a hub for all the FBI's child predator initiatives.

Mr. Chairman, Congressman Ferguson, there is no silver bullet solution to the problem of online predators. It will take the combined efforts of parents, children, law enforcement officials, and the legislature, Federal and State, to take action against these crimes. Thank you, Mr. Chairman, for permitting me to address the committee and Congressman Ferguson, for permitting me to remark on my efforts to address this issue together with each of you and the United States Congress.

[The prepared statement of Hon. Michael Fitzpatrick follows:]

PREPARED STATEMENT OF THE HON. MICHAEL FITZPATRICK, MEMBER, U.S. HOUSE OF REPRESENTATIVES

Mr. Chairman,

Thank you for inviting me to participate in today's hearing and for allowing me to give testimony on what I feel is a new and emerging problem confronting our nation's children and their safety while using the Internet. I am speaking of the rapid increase in popularity of Internet social networking sites and their use by child predators to hunt and harass our children at home, in schools and in our libraries.

As the father of six children, I know very well the challenges technology poses to our families. In a world that moves at a dizzying pace, being a father gets harder all the time. Monitoring our children's use of emerging technologies is a huge task and the Internet remains the focus of many parent's concerns.

The technological breakthrough of the World Wide Web has been enormously beneficial to society. The Internet has brought communities across the globe closer

together through instant communication. It has enabled an unfiltered free-flow of thought, ideas and opinion. The Internet has opened a window to the world right at our fingertips. However, this window opens both ways. The freedom to connect to the world anywhere at anytime brings with it the threat of unscrupulous predators and criminals who mask their activities with the anonymity the Internet provides to its users. And among its many applications, one of the most worrying developments of late has been the growth in what are known as "social networking sites."

Social networking sites like Myspace, Friendster, and Facebook have literally exploded in popularity in just a few short years. Myspace alone has almost 90 million users and ranks as the sixth most popular English language website and the eighth most popular site *in the world.*

Anyone can use these sites – companies and colleges, teachers and students, young and old all make use of networking sites to connect with people electronically to share pictures, information, course work, and common interests. These sites have torn down the geographical divide that once prevented long distance social relationships from forming, allowing instant communication and connections to take place and a virtual second life to take hold for its users.

For adults, these sites are fairly benign. For children, they open the door to many dangers including online bullying and exposure to child predators that have turned the Internet into their own virtual hunting ground. I became personally aware of the danger the Internet can pose after my 16 year old daughter began using the social networking site Myspace.com. I quickly realized that while my daughter thought she was only chatting with her friends, other people, some with criminal intent, could be looking in.

Although age limits exist on many of these sites, there is almost no enforcement of these rules. Frequently, children under the age of 16 – the cut off age for a profile on Myspace – simply lie about their age and fake being 16, 18 or even older. Predators also use this anonymity to their advantage by profiling themselves as teenagers to more easily identify and navigate the profiles of their prey.

The dangers our children are exposed to by these sites is clear and compelling. According to a study conducted by the National Center for Missing and Exploited Children (NCMEC), in 1998 there were 3,267 tips reporting child pornography. Since then, the number has risen by over 3,000 percent to an astounding 106,119 tips in 2004. The Department of Justice recognizes child pornography as a precursor for pedophiles and is often linked to online predators. According to Attorney General Gonzales, one in five children has been approached sexually on the internet. *One in five*. Worse still, a survey conducted by the Crimes Against Children Research Center found that less than one in four children told their parents about the sexual solicitation they received. Myspace, which is self regulated, has removed an estimated 200,000 objectionable profiles since it began operating in 2003. And while it is difficult to predict the exact number of total predators on the Internet at any one time, the Federal Bureau of Investigation (FBI) estimates that there are more than 2,400 active child sexual exploitation investigations under way at any given time.

This problem is finally gaining the public's attention. Look closely at local and national news stories and you will undoubtedly see a story of a crime linked to social networking sites. Recently, national news reports have focused on the case of Katherine R. Lester, a 16 year old Michigan honors student who fled to Israel with hopes of meeting a 25 year old man she met on Myspace. Two months ago, in my own congressional district, a 25 year old man, Shawn Little, was arrested for posing as a teenager online to solicit a 14 year old boy. Little's communications with the child resulted in a sexual encounter. And NBC's Dateline program has brought the threat of online predators to the televisions of millions of Americans through their acclaimed, but disturbing, "To Catch a Predator" series. While these high-profile cases make a splash on the headlines, how many other, less publicized cases of child exploitation go unnoticed?

While these stories have pressured many social networking sites to take action to improve their safety protocols, like Myspace recently has done, these changes fall short of real reform. That is why I introduced the Deleting Online Predators Act.

Parents have the ability to screen their children's Internet access at home. But this protection ends when their child leaves for school or the library. My legislation would require schools and libraries to monitor the internet activities of minors and implement technology to protect children from accessing:

1. Commercial networking sites like MySpace.com and chat rooms which allow children to be preyed upon by individuals seeking to do harm to our children; and
2. Visual depictions that are obscene or child pornography.

Preventing access to social networking sites in these situations is not designed to underestimate the importance of parental supervision. Internet safety begins at home and that is why my legislation would require the Federal Trade Commission to design and publish a unique website to serve as a clearinghouse and resource for parents, teachers and children for information on the dangers of surfing the Internet. The website would include detailed information about commercial networking sites. The FTC would also be responsible for issuing consumer alerts to parents, teachers, school officials and others regarding the potential dangers of internet child predators and their ability to contact children through MySpace.com and other social networking sites.

In addition, my Bill would require the Federal Communications Commission to establish an advisory board to review and report commercial social networking sites like MySpace.com and chat rooms that have been shown to allow sexual predators easy access to personal information of, and contact with, children.

Make no mistake; child predation on the Internet is a growing problem. Predators will look for any way to talk to children online whether through sites like Myspace, instant messaging, or even online games. The best defense against these people is to educate parents and children of the dangers that come along with the Internet and by limiting access to certain sites during the school day.

This is not all. Congress and state legislatures must also act to dedicate funds to law enforcement programs designed to combat child predators. Last month, I actively fought for and Congress passed legislation to increase funding to the FBI's Internet Crimes Against Children Task Forces and the Innocent Images National Initiative, which serves as the hub for all of the FBI's child predator initiatives. Supporting these programs will send a clear signal to child predators and pedophiles that the hunters have become the hunted and law enforcement will not relent until these criminals are apprehended.

There is no "silver bullet" solution to the problem of online predators. It will take the combined effort of parents, children, law enforcement and the legislature to take action against these crimes. Thank you, Mr. Chairman, for inviting me to address this committee and remark on my efforts to address this important issue.

I yield back the balance of my time.

MR. WHITFIELD. Congressman Fitzpatrick, thank you for your testimony and for your leadership. Speaking of MySpace, with 85 to 90 million registrants on that program, I guess, Rupert Murdoch purchased MySpace about 6 months ago for $568 million and I know they are expecting some great advertising revenues, but I am glad you brought up this whole issue of social networking. I look forward to seeing what the law enforcement people say about it, but we do know that a lot of crimes have been committed because of information obtained through the social

networking sites. And as you very correctly pointed out, there is no way to determine the age of a person that may be on that site and there is no way that can be verified.

But on your legislation that has been introduced, which committee is that? Has that been referred to Energy and Commerce?

MR. FITZPATRICK. It has been referred to the Energy and Commerce Committee and there is actually a hearing scheduled tomorrow morning for the Subcommittee on Telecommunications and the Internet.

MR. WHITFIELD. Okay. Okay, good. And under your legislation, what are the responsibilities that would be placed upon the libraries and the schools, so I can have a little bit better understanding of it?

MR. FITZPATRICK. In 2000 a law was passed by Congress and signed by President Clinton. I believe it is called the Children's Internet Protection Act. And the Children's Internet Protection Act required schools and libraries that are recipients of Federal funds for those institutions, to implement screening technology, software that would prohibit children from, while in school and in the library, accessing pornography sites. And so those schools and institutions, probably most of them in this district here, the 7th District of New Jersey, already have that technology, that software in place.

What this bill would do is require those institutions to expand the existing software, use that existing software and expand, sort of, the net to prohibit children from accessing social networking sites in these virtual chat rooms while in school or in the library, and so the technology is there. The social networking sites are a recent phenomenon, just exploding in terms of the number of users.

If you walk down the streets of this district, I am sure you would have a difficult time finding a teenager that doesn't have a profile registered and as I have spoken to parents and spoken to teachers in my district, they are as aggravated as anybody else that kids go into the computer lab, they are working on a project; they know how to access one of these networking sites or an instant messaging system and they are talking to friends in other schools, in other communities, in other States while they are in school. And so the technology is there. But essentially to answer your question, what the bill would do is take the existing technology, expand it to preclude access to social networking sites like MySpace while kids are in school.

MR. WHITFIELD. And what would be the enforcement mechanism in the bill or is there one?

MR. FITZPATRICK. Well, first, it was a question of what a social networking site is, so the bill lays out what a social networking site is and the requirement really is on the school and the library to issue a certification to the Federal government as a condition to proceed in

receiving any Federal funds. And so the mechanism would be the same as what currently exists under the Child Internet Protection Act.

MR. WHITFIELD. Well, thank you, Congressman Fitzpatrick, and I recognize Mr. Ferguson.

MR. FERGUSON. Thank you, Mr. Chairman. Thanks again for being here and I appreciate you making the long trek across the river to join us here in New Jersey. And I also appreciate your leadership on this issue. I know your concern and passion for this issue extends beyond your experience as a Member of Congress; it is as a father, as you said, and it is a concern that many of us share.

Your bill is focused on schools and libraries and we know, any of us who are parents know it is tough enough to manage or be aware of your kids' Internet use when they are at home. But of course, much of that control, much of that oversight kind of goes out the window when your kids are not in your own home. If they are at school or if they are at the library or at a friend's house--what, as you worked your bill and developed your bill, do we have any sort of statistics or evidence of how much of a problem this is in schools and libraries?

I mean, certainly we know, anecdotally, any parent will tell you their level of concern goes up when their child is not right there with them in their home. Parents have a lot of control in their own homes, but less, a lot less outside of their own home. Do we have a lot of evidence or is it mostly, is it just a sense? Is this just a, really a proactive measure to take?

MR. FITZPATRICK. Much of the evidence is anecdotal. First of all, as you point out, in the home, it is difficult enough. I mean, as a parent--we have one computer in our home that is hooked up to the Internet and it is in plain view and it kind of perplexes me and I saw a story on NBC recently with a mother shocked that her daughter was on MySpace and the content of what was on MySpace and the report was from the daughter's bedroom, so the computer was in the child's bedroom, the child goes to the bedroom, locks the door, and that is where the problem begins. But, as I testified, for purposes of my bill, it is the issue of the parents' oversight over the child while the child is at home.

But the evidence is essentially anecdotal. It is stories that we have received, it is the criminal investigations, the affidavits and probable cause that further our public record and it is a growing body of evidence that, both from law enforcement but also from school officials, the children who used to have inappropriate material accessed at school, that is not precluded on the Children's Internet Protection Act, who now have access to social networking sites while at school and in the library.

MR. FERGUSON. Well, I serve on the Telecommunications and Internet Subcommittee of this committee.

MR. FITZPATRICK. You will be there tomorrow.

MR. FERGUSON. We will be having a hearing on your bill tomorrow and I look forward to learning more about it and asking further questions at that time. Thank you, Mr. Chairman.

MR. FITZPATRICK. Thanks for your support, Congressman, appreciate it.

MR. WHITFIELD. And I am also on that Telecommunications subcommittee, so we look forward to hearing more about it tomorrow, as well.

MR. FITZPATRICK. Okay. Thank you.

MR. WHITFIELD. Thank you for being with us.

MR. FITZPATRICK. Thanks for the chance, Chairman. I appreciate it.

MR. WHITFIELD. At this time, I would like to call up the third panel which includes Mr. Frank Rodgers, who is the Lieutenant Colonel with the New Jersey State Police; Mr. Wayne Forrest, who is the Somerset County Prosecutor, Somerville, New Jersey; Mr. Anthony Ritter, who is a lieutenant with the New Jersey State Police Division Headquarters; and Mr. Andre Banks, who is a sergeant, Office of the Prosecutor for Union County in Elizabeth, New Jersey. I certainly do thank you gentlemen involved in law enforcement for being with us because you are the fellows out there on the front line and are the ones that can be most helpful to us who are trying to adopt policy in making sure we maximize our opportunity to come up with the right solutions. We recognize, also, that sometimes we interfere with the right solution, so hopefully you can lead us in the right direction, but as you have already heard, we do take testimony under oath and I am assuming none of you gentlemen have any difficulty testifying under oath, so if you would stand, I would just like to swear you in.

[Witnesses sworn.]

MR. WHITFIELD. Thank you very much. You are now under oath and Mr. Rodgers, we will recognize you for your 5-minute opening statement.

STATEMENTS OF FRANK RODGERS, LIEUTENANT COLONEL, NEW JERSEY STATE POLICE; WAYNE FORREST, ESQUIRE, SOMERSET COUNTY PROSECUTOR; ANTHONY RITTER, LIEUTENANT, NEW JERSEY STATE POLICE; ANDRE BANKS, SERGEANT, OFFICE OF THE PROSECUTOR, UNION COUNTY, NEW JERSEY

MR. RODGERS. Good morning, Mr. Chairman, Mr. Ferguson and members of the subcommittee. I am Lieutenant Colonel Frank Rodgers,

the Deputy Superintendent of Investigations for the New Jersey State Police. I appreciate the opportunity to discuss with you how the State of New Jersey is combating predators on the Internet.

I have been a member of the New Jersey State Police for 25 years and involved in criminal investigations for 21 of those years. Never in my career have I seen criminal activities as far reaching or rapid in growth as Internet related crimes. Never have I witnessed crimes so egregious and so prevalent as those being committed against the youth of New Jersey and all across America right in their own homes.

As the Deputy Superintendent of the Investigations Branch, I am privileged to command 800 fine men and women assigned to the Intelligence Section, the Special Investigations Section, and the Office of Forensic Science. As the commander of this Branch, under the leadership of Colonel Rick Fuentes, the Superintendent of the New Jersey State Police, we are reshaping how law enforcement does business in the State of New Jersey.

Last year the New Jersey State Police operationalized an intelligence Led policing strategy. In doing so, we adopted the processes intrinsic to that strategy; most importantly, intelligence sharing. At present, we have deployed our Statewide Intelligence Management System, which is known as SIMS, to 300 of the State's 600 police departments, including the FBI. We are currently working with our law enforcement allies to network this system to others around the State and region to fill in the holes. We have also initiated a full-time all crimes, all hazards intelligence fusion center at our headquarters in West Trenton.

That center will expand dramatically in September, when we open with our many allied law enforcement, intelligence, and other public safety partners, what will be the largest and most sophisticated intelligence fusion center in the country. The 55,000 square foot Regional Operations and Intelligence Center, known as the ROIC, embodies our commitment to the fundamental recommendations of both the 9/11 Commission and the National Intelligence Sharing Plan, unity of effort and true intelligence sharing.

The New Jersey State Police has been fighting Internet predators for 10 years. We are proud to work with our many partners on these critical investigations. To give you an idea of our commitment over the last 10 years, our team has averaged over 100 Internet related child exploitation investigations each year and has averaged 45 arrests a year for the victimization of children over the Internet.

We are proud and honored to be selected as the primary agency in New Jersey to lead the New Jersey Internet Crimes Against Children Task Force, known as ICAC. We have concentrated our mission into three main areas; training, outreach, and enforcement. We currently

have 20 cyber investigators on our task force, 10 of which hunt Internet predators full time. Thanks to ICAC funding, we have been able to send these individuals to 120 training events over the last 18 months; technical training that is key to doing the job. This never would have been possible without ICAC funding.

Over the last 18 months we have conducted 310 presentations to over 30,000 students, teachers, parents, and law enforcement officials from across this State. We are currently working to expand cooperation and information sharing through the New Jersey Department of Education, the New Jersey Education Association, the New Jersey Parent Teacher Association, and the New Jersey Association for Educational Technology. Educating the children must come from all fronts and it must come loud and often.

Finally, I would like to speak to you briefly about enforcement. These programs are working and we are making a difference. Could we do more? Certainly. And we ask your support in helping us get there. However, from the many challenges that we face, we have accumulated many accomplishments. Most recently, during the week of June 26, 2 weeks ago, members of the New Jersey Internet Crimes Against Children Task Force, in partnership with 20 other law enforcement agencies around the State, arrested seven individuals for the possession and distribution of child pornography over the Internet.

The arrests were a result of a 3-month undercover investigation and they included an elementary school teacher, a medical intern about to begin his residency, and a resident of Bridgewater, New Jersey, right here in Somerset County. The techniques used to capture these individuals were provided through ICAC training.

On March 3 of this year, task force members, in conjunction with members of the FBI Innocent Images, arrested a 33-year old subject for sexually assaulting a 14-year old who he met through MySpace.com. This subject traveled to Florida while the victim was there on vacation with her family, sexually assaulted her, and then returned with her to New Jersey, knocked on the front door of the residence where the young lady lived and professed his love to the parents at the door.

This time last year, over a 9-day period, as a result of an investigation which we dubbed Operation Guardian, following up on leads provided to us by the Wyoming ICAC, the New Jersey ICAC Task Force members arrested 39 individuals for possession and distribution of child pornography over the Internet. Included in these arrests were a defense attorney, a high school teacher, and a pediatric neurosurgeon.

Finally, going back a couple years, through the results of information provided to us by the Dallas ICAC in conjunction with the FBI and a matter prosecuted by Mr. Christie's office, a former Superior Court judge

from Camden County was charged with endangering the welfare of a child after we executed a search warrant on two of his homes and his office. Following up on this ICAC evidence, during the searches we uncovered a videotape depicting this judge engaged in sexual activity with a 10-year old Russian juvenile. The subject is currently incarcerated in a Federal prison.

As you can imagine, I could go on and on with regard to these cases. Our experience shows us these child predators will continue to prey upon the most innocent and vulnerable members of our society, our children. We ask your continued support for our mission and we assure you that we remain committed to the children of New Jersey by arresting those individuals who are prowling the Internet every day for a new victim. Thank you.

[The prepared statement of Frank Rodgers follows:]

PREPARED STATEMENT OF FRANK RODGERS, LIEUTENANT COLONEL, NEW JERSEY STATE POLICE

1. Introduction
   a. 25 years law enforcement experience, 21 years in criminal investigations
   b. Commander of 800 fine men and women

2. New Direction
   a. Leading a Branch reorganization based on intelligence led policing
   b. Deployed a statewide intelligence management system
   c. Initiated a full time, all crimes intelligence fusion center

3. Resource Sharing
   a. Must be inclusive of all local, county, state and federal law enforcement partners

4. New Jersey Internet Crimes Against Children (ICAC) Task Force
   a. Training
      1) 20 cyber investigators on task force
      2) Investigators have attended 120 training events in the last 18 months
   b. Outreach
      1) 310 presentations have been given in the last 18 months
      2) Expanding capabilities with education partners
   c. Enforcement
      1) List of five case histories

5. Conclusion
   a. Successful track record in task force leadership
   b. Continued commitment to the ICAC mission

Good morning Mr. Chairman, Ranking Member Stupak and members of the Subcommittee, I am Lieutenant Colonel Frank Rodgers, Deputy Superintendent of the Investigations Branch of the New Jersey State Police. I appreciate the opportunity to discuss with you how the State of New Jersey is Combating Predators on the Internet.

I. Introduction

I have been a member of the New Jersey State Police for the last 25 years and have been involved in criminal investigations for 21 of those 25 years. Never in my career have I seen criminal activities as far reaching or rapid in growth as Internet related crimes. Never have I witnessed crimes so egregious and so prevalent as those being committed against the youth of New Jersey and youth all across America right in their own homes.

As Deputy Superintendent of the Investigations Branch, I am privileged to command the 800 fine men and women of the Intelligence Section, the Special Investigations Section and the Office of Forensic Science of the New Jersey State Police. As commander of this Branch, under the leadership of Colonel Rick Fuentes, Superintendent of the New Jersey State Police and with oversight and endorsements from both our Attorney General Zulima Farber and Governor Jon Corzine, we are reshaping how law enforcement does business in the State of New Jersey.

II. A New Direction

Last year the New Jersey State Police operationalized an Intelligence Led Policing strategy. In doing so we adopted the processes intrinsic to that strategy, most importantly, intelligence sharing. At present we have deployed our Statewide Intelligence Management System (SIMS) to 300 of the state's 600 police departments, including the FBI. We are currently working with our law enforcement allies to network this system to others around the state and region to fill in the holes. We have also initiated a full time all crimes all hazards intelligence fusion center at our headquarters in West Trenton. That center will expand dramatically in September when we open with our many allied law enforcement, intelligence and other public safety partners, what will be the largest and most sophisticated intelligence fusion center in the country. The 55 thousand square foot Regional Operations and Intelligence Center known as the ROIC embodies our commitment to the fundamental recommendations of both the 911 commission and the National Intelligence Sharing Plan, unity of effort and true intelligence sharing.

III. Resource Sharing

We have all heard the phrases "surfing the Internet" or "surfing the web" and I must admit it gives one the connotation of fun, freedom, adventure and excitement. Who wouldn't want to "surf the net"? We all do it and we all enjoy it. Yet as we are all too well aware, at least those of us in this room, there are sharks in the water and riptides waiting to pull our children out to sea. We are committed to protecting our children from the dangers of the Internet and we have been very successful thus far. But like everyone else who takes the oath to protect and serve, we cannot do it alone, this is bigger than any one agency, any one state. We are a team made up of local, county, state and federal partners and we ask for your continued support.

The New Jersey State Police has been fighting Internet predators for the last ten years. We are a multi-faceted organization with a strong reputation, intense work ethic and unwavering integrity. We are proud to work with our many partners on these critical investigations. To give you an idea of our commitment over the last ten years, our team has averaged 100 Internet related investigations a year and we average 45 arrests per year for the victimization of children through the Internet.

IV. New Jersey Internet Crimes Against Children (ICAC) Task Force

We are proud and honored to be selected as the primary agency in New Jersey to run the New Jersey Internet Crimes Against Children Task Force (ICAC). We have concentrated our mission into three main areas: training, outreach and enforcement.

A. Training

We currently have 20 cyber investigators on our task force, 10 of which hunt Internet predators full time. Thanks to ICAC funding, we have be able to send these individuals to 120 training events over the last 18 months, technical training that is key to doing the job. This would never have been possible without ICAC funding.

B. Outreach

Over the last 18 months we have conducted 310 presentations to over 30,000 students, teachers, parents and law enforcement officials across the State. We are currently working to expand cooperation and information sharing through the New Jersey Department of Education, the New Jersey Education Association, the New Jersey Parent Teacher Association and the New Jersey Association for Educational Technology. Educating the children must come from all fronts and it must come loud and often.

C. Enforcement

Finally, I would like to speak to you about enforcement. These programs are working, we are making a difference. Can we do more? Yes of course, and we ask for your support in getting us there. However, through all the challenges and horrors that we face, we have made bold accomplishments.

Case # 06-06

During the week of June 26, 2006, members of the New Jersey Internet Crimes Against Children Task Force in partnership with 20 other law enforcement agencies throughout the State, arrested seven individuals for the possession and distribution of child pornography over the Internet. The arrests were as a result of a three month undercover investigation and included an elementary school teacher, a medical intern about to begin his residency, an enlisted member of the United States Coast Guard and a resident of Bridgewater, New Jersey right here Somerset County. The techniques used to capture these individuals were provided through ICAC training.

Case # 06-24

On March 3, 2006, task force members in conjunction with members from FBI Innocent Images arrested a 33 year old man for sexually assaulting a 14 year old girl whom he had met through myspace.com. He traveled to Florida while she was there on vacation with her family, sexually assaulted her in Florida and then traveled to New Jersey after they returned home, knocked on their front door in order to meet her parents and professed his love for their daughter.

Case #04-39

Over a nine day period in January, 2005 and as a result of leads from the Wyoming ICAC, the New Jersey ICAC task force arrested 39 individuals for possession and distribution of child pornography over the Internet. Arrests included a defense attorney, a high school teacher and a pediatric neurosurgeon.

Case # 03-08

In August 2003, as a result of leads from the Dallas ICAC and in conjunction with the FBI and the United States Attorney's Office, a former Camden County Superior Court Judge was federally charged with Endangering the Welfare of a Child as a result of the execution of search warrants on his two homes and office. During the searches, detectives uncovered a video tape recording of the judge having sex with a Russian male juvenile. He is currently serving a ten year term in federal prison.

V. Conclusion

As you can imagine these stories go on and on. Our experience shows us that these child predators will continue prey upon the most innocent and vulnerable members of our society. We ask that you continue to support our mission, as we remain committed to the children of New Jersey by identifying and arresting those who are prowling the Internet everyday for a new victim.

MR. WHITFIELD. Thank you, Mr. Rodgers. And Mr. Ritter, you are recognized for your 5-minute opening statement.

MR. RITTER. Good morning, Mr. Chairman, Congressman Ferguson. I am Lieutenant Anthony Ritter, Assistant Bureau Chief of the Computer Crimes and High Technology Surveillance Bureau within the Special Investigations Section of the New Jersey State Police. I appreciate the opportunity to discuss with you our issues regarding combating predators on the Internet. I have been a member of the New Jersey State Police for 22 years and have been involved in both technology and cyber investigations for the last 17 years. The Computer Crimes and High Technology Surveillance Bureau coordinates the efforts of the New Jersey Internet Crimes Against Children Task Force. I would like to address some of the challenges that face our task force and that of cyber law enforcement in general.

First, data retention. There has been much testimony before the committee on the subject of data retention by Internet service providers and I would like to address three major concerns brought forth by the ISPs, generally. First, the ISPs are not clear who will be able to access records of someone's online behavior. The law enforcement process begins with reasonable suspicion to develop required probable cause and operates under legal guidance and court orders. I think unauthorized insider access to records is of graver concern to the ISPs.

Second, the ISPs are not clear who would pay for the data warehousing of these additional records. I think everyone will bear a part of that cost. And third, ISPs say it is not clear that police are hindered by the current law as long as they move swiftly in the investigative process. In this case, they may be partly correct. There needs to be a consistent, measured approach to data retention and an increase in the speed of the investigative process. We both must work more efficiently.

Although we are pleased to see the ISPs moving forward voluntarily to address our concerns where they can, we seek to have a standard established for the retention of data by ISPs. All ISPs should be required to have the capability of isolating targeted traffic and upon the receipt of a court order, deliver that content to a law enforcement monitoring facility in a standardized manner. This capability needs to extend to all methods of communication services supported by this industry.

Quality of service. Quality of service is an industry-recognized term that is important to a business's ability to maintain and increase its customer base. In our case, law enforcement is the customer and poor customer service equates to a delayed law enforcement action. These delays can result in an inability to continue investigative leads in a timely manner. Our goal here is to institute industry-wide standards to ensure

the efficient and timely return of the information sought by law enforcement.

Cost. There is an explosion in technology and it is the convergence of telephony networks and data networks on portable data assistants, known as PDAs, cell phones, and other wireless devices. Current costs for intercepting conventional wireless devices can reach as much as $2,600 per intercept order. Our fear is that the cost associated with IP intercept will exceed the cost of conventional intercept and will price many law enforcement agencies out of this investigative crime fighting tool.

Personnel. The need for skilled investigators is as critical as data retention. Without the data we cannot investigate; without the detective, we cannot investigate. In New Jersey's Peer-to-Peer initiative, we have over 83,000 leads. As Lieutenant Colonel Rodgers stated, we have 10 full-time detectives with half working proactively. The other half are working reactively on referrals and direct complaints. And what about being proactive in the other areas of the Internet? Most people only know of browsing the Web, but there are many other ways of communicating across the Internet and each one could keep a whole squad of detectives busy 24 hours a day.

Tools. Additional research and development needs to be conducted by law enforcement, technology corporations, and institutions of higher learning to close the large gaps impeding our ability to fight technology crime against Internet predators. We need to collect technical data and present it in an easy to view graphical format. We need to automate the process of locating network log files regardless of an operating system. We need to overcome the obstacles of anonymizers, IP spoofing, encrypted data, and steganography. We need to forensically capture a computer's Random Access Memory or RAM without modification or alteration.

We need to provide real time IP intercept on data networks in a standardized format with the ability to isolate the target and capture the communication inclusive of all activities, such as instant messaging, voice over IP phone calls, webcams, e-mail, and Web browsing. We need to facilitate an automated and standardized stored data handover interface for the return of historical records requested by subpoena or court order. And we need to develop tools to locate the physical position of devices connected to wireless networks.

Solutions. There have been many suggestions by the men and women fighting Internet crimes against children in New Jersey and ways to improve and streamline our mission. Here are some of their thoughts. Increase ISP record retention to not less than 2 years to include, but not

be limited to, subscriber information, method of payment, types of devices connected and all in and out IP logging records.

Mandate that out-of-state subpoenas and warrants be recognized as valid legal documents. Create a website rating system much like the one used by the motion picture industry so parents can more easily block content. Sponsor a national Internet safety campaign through television and movie theaters. Evaluate the Counterdrug Technology Assessment Center's, CTAC, technology transfer program and model a similar program to support agencies combating Internet predators.

Recognize the FCC's Second Report and Order and Memorandum Opinion and Order that addresses several issues regarding the implementation of the Communications Assistance for Law Enforcement Act, CALEA, enacted in 1994. The primary goal of the order is to ensure that law enforcement agencies have all the resources that CALEA authorizes, particularly with regard to facilities-based broadband Internet service providers and interconnected voice over Internet protocol or VOIP providers. Although the VOIP issue has now been addressed, other packet-based services such as instant messaging, picture messaging, and a host of other Internet-based communication services have been excluded from CALEA standards. This needs to be corrected.

Endorse and support and promote the expansion and implementation of Internet Protocol version 6 (IPv6), which will allow ISPs the ability to give every Internet accessible device its own unique static IP address and eliminate the nightmare of dynamic IP addressing issues. The United States government has specified that network backbones of all Federal agencies must deploy IPv6 by the year 2008.

With the proper resources, States can and will do much more to continue the fight against Internet predators. We remain committed to maintaining existing operations without minimization and are honored to be a partner in the fight against Internet child victimization.

[The prepared statement of Anthony Ritter follows:]

PREPARED STATEMENT OF ANTHONY RITTER, LIEUTENANT, NEW JERSEY STATE POLICE

1. Introduction
   a. 22 years law enforcement experience
   b. Oversees operation of the New Jersey Internet Crimes Against Children Task Force

2. Challenges
   a. Data Retention
      1) Need to establish standards for data retention
      2) Should apply to all methods of communication services
   b. Quality of Service
      1) Need for industry wide standards for return of information to law enforcement

c. Costs
   1) Costs for intercept of data may prove prohibitive
d. Personnel
   1) There is a serious lack of skilled investigators
e. Tools
   1) Development of additional investigative technology tools is needed

3. Solutions
   1) Increase ISP record retention without limitations
   2) Recognition of out-of-state subpoenas and warrants
   3) Institute a website rating system
   4) Sponsor a national Internet Safety campaign
   5) Empower technology transfer programs to provide needed tools
   6) Expand CALEA to fully support all IP based communication services
   7) Support rapid deployment of IPv6

Good morning Mr. Chairman, Ranking Member Stupak and members of the Subcommittee, I am Lieutenant Anthony Ritter, Assistant Bureau Chief of the Computer Crimes and High Technology Surveillance Bureau within the Special Investigations Section of the New Jersey State Police. I appreciate the opportunity to discuss with you our issues regarding combating predators on the Internet.

I. Introduction

I have been a member of the New Jersey State Police for 22 years and have been involved in both technology and cyber investigations for the last 17 years. The Computer Crimes and High Technology Surveillance Bureau which coordinates the efforts of the New Jersey Internet Crimes Against Children (ICAC) Task Force.

II. Challenges

I would like to address some of the challenges that face our task force and that of cyber law enforcement in general.

A. Data Retention

There has been much testimony before the committee on the subject of data retention by Internet Service Providers (ISPs) and I would like to address the three major concerns brought forth by ISPs generally. First, the ISPs are not clear who will be able to access records of someone's online behavior. The law enforcement process begins with reasonable suspicion to develop required probable cause and operates under legal guidance and court orders. I think unauthorized insider access to records is of graver concern to the ISPs. Second, the ISPs are not clear who would pay for the data warehousing of these additional records. I think everyone will bear part of the cost. And third, ISPs say it is not clear that police are hindered by current law as long as they move swiftly in the investigative process. In this case, they may be partly correct. There needs to be a consistent, measured approach to data retention and an increase in the speed of the investigative process. We both must work more efficiently. Although we are pleased to see the ISPs moving forward, voluntarily, to address our concerns where they can, we seek to have a standard established for the retention of data by ISPs. All ISPs should be required to have the capability of isolating targeted traffic and upon receipt of a court order, deliver that content to a law enforcement monitoring facility in a standardized manner. This capability needs to extend to all methods of communication services supported by this industry.

B. Quality of Service

Quality of service is an industry recognized term that is important to a business's ability to maintain and increase its customer base. In our case, law enforcement is the customer and poor customer service equates to a delayed law enforcement action. These delays can result in an inability to continue investigative leads in a timely manner. Our goal here is to institute industry wide standards to ensure the efficient and timely return of the information sought by law enforcement.

C. Costs

There is an explosion in technology and it is the convergence of telephony networks and data networks on portable data assistants (PDA), cell phones and other wireless devices. Current costs for intercepting conventional wireless devices can reach as much as $2600 per intercept order. Our fear is that the costs associated with IP intercept will exceed the costs of conventional intercepts and will price many law enforcement agencies out of this investigative crime fighting tool.

D. Personnel

The need for skilled investigators is as critical as data retention. Without the data we cannot investigate, without the detective we cannot investigate. In New Jersey's Peer-to Peer (P2P) initiative we have over 83,000 leads and as LTC Rodgers stated, we have 10 full time detectives with half working proactively. The other half are working reactively on referrals and direct complaints. And what about being proactive in other areas of the Internet? Most people only know of browsing the web, but there are many other ways of communicating across the Internet and each one could keep a whole squad of detectives busy 24 hours a day.

E. Tools

Additional research and development needs to be conducted by law enforcement, technology corporations, and institutions of higher learning to close the large gaps impeding our ability to fight technology crime against Internet predators. We need to:

- collect technical data and present it in an easy to view graphical format.
- automate the process of locating network log files regardless of operating system.
- overcome the obstacles of anonymizers, IP spoofing, encrypted data and steganography.
- forensically capture a computer's Random Access Memory (RAM) without modification or alteration.
- provide real time IP intercept on data networks in a standardized format, with the ability to isolate the target and capture the communication inclusive of all activities such as instant messaging, voice over IP phone calls, web cams, emails and web browsing.
- facilitate an automated and standardized stored data handover interface for the return of historical records requested by subpoena or court order.
- develop tools to locate the physical position of devices connected to wireless networks.

III.Solutions

There have been many suggestions from the men and women fighting Internet Crimes Against Children in New Jersey on ways to improve and streamline our mission. Here are some of their thoughts:

A. Increase ISP record retention to not less than two years to include, but not be limited to, subscriber information, method of payment, types of devices connected and all in and out IP logging records.

B. Mandate that out-of-state subpoenas and warrants be recognized as valid legal documents.

C. Create a website rating system much like the one used by the motion picture industry so that parents can more easily block content.
D. Sponsor a national Internet Safety campaign through television and movie theaters.
E. Evaluate the Counterdrug Technology Assessment Center's (CTAC) technology transfer program and model a similar program to support agencies combating Internet predators.
F. Recognize the FCC's *Second Report and Order and Memorandum Opinion and Order* that addresses several issues regarding implementation of the Communications Assistance for Law Enforcement Act (CALEA), enacted in 1994. The primary goal of the *Order* is to ensure that Law Enforcement Agencies have all of the resources that CALEA authorizes, particularly with regard to facilities-based broadband Internet Service Providers and interconnected voice over Internet Protocol (VOIP) providers. Although the VOIP issue has now been addressed, other packet based services such as instant messaging, picture messaging and a host of other Internet based communication services have been excluded from CALEA standards. This needs to be corrected.
G. Endorse, support and promote the expansion and implementation of Internet Protocol version 6 (IPv6) which will allow ISPs the ability to give every internet accessible device its own unique static IP address and eliminate the nightmare of dynamic IP addressing issues. The United States Government has specified that the network backbones of all federal agencies must deploy IPv6 by 2008.

IV. Conclusion

With the proper resources, states can and will do much more to continue the fight against Internet predators. We remain committed to maintaining existing operations without minimization and are honored to be a partner in the fight against Internet child victimization.

MR. WHITFIELD. Thank you, Mr. Ritter. At this time, Mr. Forrest, you are recognized for 5 minutes.

MR. FORREST. Thank you, Mr. Chairman, Congressman Ferguson. Good morning. My name is Wayne Forrest. I am the prosecutor here in Somerset County. New Jersey has 21 counties, 21 county prosecutors. I have been serving as our county prosecutor for the past 9 years. Prior to that I worked in the Attorney General's office and in total I have over 30 years in law enforcement. In addition to that, I am an adjunct professor here at this college where I have been teaching for the past 15 years and along with a colleague of mine, Prosecutor Barnes from Hunterdon County, we moved our regional police academy to this institution, as well. So we welcome you here and if you have more time, we will give you a tour of our police academy before the end of the day.

Like the rest of the country, over the past 10 years we in Somerset County have also experienced a dramatic increase in cases involving sexual exploitation of children. Our experience shows that this increase is due large in part to the proliferation of the Internet. In Somerset County in particular, I believe we have had extensive experience with

this problem because Somerset County is such an affluent county. In fact, in the year 2000 U.S. census ranked Somerset County as the number one county in the country in median household income at $88,957.

As a wealthy county, computers are everywhere in Somerset County. All Somerset County children have access to the Internet, either at home, at school, at the library, at a friend's house. And in addition, Somerset County children also have more privacy and autonomy due to the factors such as both parents being employed outside the home, larger homes with individual bedrooms for each child and frequently, a personal computer with Internet access in the bedrooms. Under these circumstances, the sexual exploitation of children over the Internet is of particular concern to us in Somerset County.

As an aside, when I came up to Somerset County from Trenton to become the prosecutor in 1997, I met with the then U.S. Attorney who introduced me, for the first time, to the Federal initiative, Innocent Images, which is what we have heard talked about before. As a parent, I was somewhat alarmed and immediately went back to the freeholders and said I feel the need to dedicate one of our detectives full time to this initiative. It is hard for local prosecutors and local freeholders to understand that you have to send someone elsewhere and how that is going to benefit your county and the economic impact on that.

We did that and I began learning, myself, as a parent, the dangers of the Internet and at the same time we sent detectives to the State Police initiative, which began back at the same time as the high tech crimes unit. We had two detectives, for a period of 6 or 7 years, outside of Somerset County learning, educating themselves, and at the same time making cases with those initiatives that came back to Somerset County. When I first did that, a number of my colleagues who were prosecutors at the time, my freeholders who finance our office, said why Somerset County? Why are you doing it? Why not one of the bigger counties? Why shouldn't they be doing it? And the reason I gave them is what I just said, because in Somerset County, you come to my neighborhood, every house has computers on every floor. Kids have personal computers, laptops; they are all over the place. Far more prolific than in other counties.

Having been in law enforcement now for over 30 years, I can tell you that 30 years ago there were far less cases involving the sexual exploitation of children. At that time, pedophiles interested in sexual activity with children would have to leave the privacy and security of their own homes to physically trade child pornography with other likeminded individuals or lurk at the schoolyard fence and attempt to lure an actual child victim. Now what we have seen is that through the Internet, pedophiles have access to millions of images, child

pornography from all over the globe without even leaving their bedrooms.

In addition, the prolonged viewing of unlimited and readily available child pornography leads to more and more pedophiles to take the next step and to attempt to meet and victimize an actual child. Our experience in Somerset County, small, affluent Somerset County, has taught us that this type of criminal behavior is happening every day and generally falls into one of three main categories: one, cases involving actual child victims who are sexually assaulted; two, cases involving undercover agents posing as child victims, which is the Innocent Images initiative, who are solicited online for sexual activity; and three, child pornography cases.

In Somerset County, while we have always had cases involving actual child victims who are sexually assaulted, the Internet has led us to an increase in cases in which the child victim willingly participates in the initial contact with the pedophile. Due to the pedophile's ability to groom the child victim over time through repeated communications over the computer, our experience has shown us that the child victim will begin to identify with the offender and be more willing to meet with that offender.

Some examples of Somerset County cases. One example is the Christopher Wahler case. And what you will see in all our cases, I provide them in our written statement, the profile of the individual that we see is someone like us; middle age, 30s, 40s, 50s; usually affluent; usually a family man; usually a man; good job; and that is what we have here. I believe Defendant Wahler came from Upper Saddle River, another affluent community. He is a 36-year old man, met with a 14-year old victim over the Internet. He posed as a 17-year old boy; was able to get her to trust him. Through repeated communications with the victim, he convinced the victim to meet with him, in person, at which time he sexually assaulted her here in Somerset County.

With regard to cases involving undercover agents posing as children who are targets of pedophiles, who engage them in graphic sexual communications over the Internet and subject them to images of pornography, we have found that pedophiles do not hesitate to travel to our county to meet their intended victims in person for sexual activity. Some of the many cases, again, that I had cited in my written statement, two include the Marc Balkin case and the Edward Bostonian case, described in greater detail in the written statement. But in addition, our experience shows that this type of offender often exhibits no signs of being a danger to children prior to their arrest, which is demonstrated by the fact that we have arrested professionals, teachers, and even a police officer for these types of offenses.

Finally, the prevalence of computers in Somerset County brings with it the concomitant presence of child pornography. As with any community in which there are computers with Internet access, there are individuals in Somerset County who use their computers to view, download, transmit or create child pornography, as evidenced by the cases of James Nafus, Jr. and Christopher Hickman, cases I have also included in my written statement.

After recognizing the growing nature of this problem approximately 10 years ago, when I left the Attorney General's office to become the Somerset County prosecutor, I took a number of steps to educate and train our police officers, system prosecutors, and most importantly, the parents in our county in an effort to combat this problem and protect the citizens of Somerset County. For example, in 1998 we created a free Internet safety presentation that educates parents and other concerned citizens on the dangers of the Internet and provides guidance for keeping children safe.

We also created and distributed free informational brochures for parents and children and provide rules for Internet use. We have copies, sample copies of the brochures for both of you, as well as a mouse pad that we provide to children and parents that we distributed throughout the schools. That is also on our website. In addition, I have sent our assistant prosecutors and detectives for advanced training in investigating and prosecuting these types of crimes so that we can stay at least one step ahead of individuals who commit these crimes in the constantly changing area of computer technology and computer crimes.

Finally, I created a High Tech Computer Crimes Unit within the prosecutor's office to assist other law enforcement agencies in properly investigating these specialized crimes. Through these steps, I believe the Somerset County Prosecutor's Office provides the citizens of Somerset County with highly trained police officers and detectives to both proactively and reactively investigate these more challenging crimes, assistant prosecutors who are better prepared to prosecute these cases, and the educational awareness to help prevent the sexual exploitation of our children over the Internet.

I recognize that we cannot win this war alone here in Somerset County. This war goes well beyond our territorial boundaries. In fact, it is international. You were questioning the U.S. Attorney about Federal jurisdiction; it is beyond that. As I said, I have been in law enforcement over 30 years and this is, I believe, the most challenging type of crime that I have ever confronted. I thank you for your interest and I thank you for time today.

[The prepared statement of Wayne J. Forrest, Esq., follows:]

PREPARED STATEMENT OF WAYNE J. FORREST, ESQ., SOMERSET COUNTY PROSECUTOR, OFFICE OF THE SOMERSET COUNTY PROSECUTOR

Dear Honorable Members of the United States House of Representatives:

In the past ten years we here in Somerset County have experienced a dramatic increase in cases involving the sexual exploitation of children. Our experience shows that this increase is due in large part to the proliferation of the Internet. In Somerset County in particular, I believe we have had extensive experience with this problem because Somerset County is such an affluent county. In fact, the 2000 United States Census ranked Somerset County as the number one county in the country in median household income at $88,957.00. As a wealthy county, computers are everywhere in Somerset County. All Somerset County children have access to the Internet, either at home, at school, at the library, or at a friend's house. In addition, Somerset County's children also have more privacy and autonomy due to factors such as both parents being employed outside the home, large homes with individual bedrooms for each child, and frequently a personal computer with Internet access in their bedroom. In addition, because these crimes ordinarily require privacy and money to purchase expensive computer equipment, Somerset County residents, who due to their wealth generally possess more of each, are in a better position than the average citizen to commit these types of offenses. Under these circumstances, the sexual exploitation of children over the Internet is of particular concern to us in law enforcement in Somerset County.

Having been in law enforcement now for over thirty years, I can tell you that thirty years ago, there were far fewer cases involving the sexual exploitation of children. At that time, pedophiles interested in sexual activity with children would have to leave the privacy and security of their homes to physically trade child pornography with other like-minded individuals or "lurk" at the schoolyard fence in an attempt to lure an actual child victim. Now, what we have seen is that through the Internet, pedophiles have access to millions of images of child pornography from around the globe without leaving their homes or workplace. For some, the ubiquity of, and ease with which they can obtain child pornography, feeds on itself until that interest consumes more and more of their daily lives. At that point, photographs cease to be enough, and the pedophile takes the next step and seeks out an actual child to victimize. The Internet then assists those pedophiles in finding an actual child victim as well. Through the Internet, a pedophile can search for an actual child victim, gather personal information or other intelligence on that victim through various search engines, and ultimately, make contact with a child victim under false pretenses. For example, a pedophile can now research an intended victim through the victim's profile or "blog," and determine that victim's photograph, age, phone number, email address, physical address, school, employer, siblings, friends, interests, likes and dislikes. Then, once armed with a wealth of information about that victim, the pedophile can make contact with the victim through an instant message using an assumed identity. Instead of "Joe Child Molester," 50 year-old registered sex offender, he can contact the victim as 16 year-old "Billy," a friend of the victim's friend Jessica, who saw the victim at the movies last Friday night and thinks she's cute. Because the contact is not face-to-face, and because the victim now believes that she is communicating with a peer, she will open-up more quickly and give more information to the pedophile. Through this process, the pedophile can "groom" the victim, and ultimately exploit his knowledge of the victim to obtain an in-person meeting with the victim.

Our experience in Somerset County has taught us that this type of criminal behavior is happening every day, and generally falls into one of three main categories: (1) cases involving actual child victims who are sexually assaulted; (2) cases involving undercover agents posing as children ("virtual victims") who are solicited online for sexual activity, and (3) child pornography cases.

In Somerset County, while we have always had cases involving actual child victims who are sexually assaulted, the Internet has led to an increase in cases in which the child victim willingly participates in the initial contact with the pedophile. Due to the pedophile's ability to "groom" the child victim over time through repeated communications over the computer, our experience shows that the child victim will begin to identify with the offender and be more willing to meet that offender in person. One example of this is the Christopher Wahler case, described in detail below, in which a 36 year-old man met a 14 year-old victim over the Internet by posing as a 17 year-old boy. Through repeated communications with the victim, he convinced the victim to meet him in person, at which time he sexually assaulted her.

With regard to cases involving undercover agents posing as children who are the targets of pedophiles who engage them in graphic sexual communications over the Internet and subject them to images of pornography, we have found that pedophiles do not hesitate to travel to Somerset County to meet their intended victims in person for sexual activity. Some examples of these types of cases are the Marc S. Balkin and Edward Bostonian cases described in detail below. In addition, our experience shows that this type of offender often exhibits no obvious signs of being a danger to our children prior to his arrest, which is demonstrated by the fact that we have arrested professionals, teachers, and even a police officer for this type of offense.

Finally, the prevalence of computers in Somerset County brings with it the concomitant presence of child pornography. As with any community in which there are computers with Internet access, there are individuals in Somerset County who use their computers to view, download, transmit or create child pornography, as evidenced by the James Nafus, Jr. and Christopher Hickman cases described below.

The following case summaries are some of the investigations and prosecutions conducted by the Somerset County Prosecutor's Office involving the sexual exploitation of children over the Internet over the past ten years.

Cases with Actual Victims

State v. Christopher D. Wahler. Case No. 97-635 / Ind. No. 98-01-00039-I. In the fall of 1997, 36 year-old defendant Christopher Wahler met a 14 year-old Bernards Township girl in an America On-Line chat room. While the victim was using a friend's computer, she received an instant message from "Steven," later determined to be defendant. Defendant claimed to be a 17 year-old boy and developed an online friendship with the victim. This friendship led to telephone calls and eventually, in-person meetings. On three occasions, defendant drove to Bernards and engaged in vaginal, oral and anal intercourse with the victim in the back of his van in the parking lot of her condominium complex. On June 16, 1998, defendant pled guilty to 3 counts of 2nd degree sexual assault and on January 8, 1999, was sentenced to six years in New Jersey State Prison. Defendant was paroled from Northern State Prison on September 16, 2002.

State v. Christopher Sopko. Case No. 04-358 / Ind. No. 04-07-00483-I. In spring 2003, 20 year-old defendant Christopher Sopko met and began communicating with a 14 year-old Branchburg girl via America On-Line Instant Messenger. Thereafter, defendant Sopko met with the victim in-person and engaged in sexual intercourse with her. On August 23, 2004, defendant pled guilty to one count of 2nd degree sexual assault and on May 13, 2005 was sentenced to three years New Jersey State Prison.

State v. Carl Niro, Jr. Case No. 05-495 / Ind. No. 05-07-00592-I. In June 2005, 22 year-old defendant Carl Niro, Jr., met a 15 year-old victim through her "My Space" website. Thereafter, defendant Niro picked the victim up at her school and drove her to his Raritan Borough residence, where he engaged in vaginal and anal intercourse with her. On March 17, 2006, defendant Niro pled guilty to 3rd degree endangering the welfare of a child, and is currently awaiting sentencing.

State v. Michael Capone. Case No. 05-518 / Ind. No. 05-07-00618-I. In summer, 2005, 24 year-old defendant Michael Capone met a 15 year-old victim through her "My Space" website. In June 2005, the 15 year-old girl was reported missing by her guardian. The ensuing police investigation revealed that on two occasions in the summer, 2005, defendant Capone picked the victim up, took her to his residence, and engaged in sexual intercourse with her. On January 6, 2006, defendant Capone pled guilty to 2nd degree sexual assault and 3rd degree endangering the welfare of a child, and is currently awaiting sentencing.

Cases with "Virtual" Victims

State v. Marc S. Balkin. Case No. 99-100 / Ind. No. 99-05-0290-I. In winter, 1999, 51 year-old defendant Marc Balkin met an undercover agent posing as a 14 year-old girl in an online chat room entitled "barely legalf4olderm." The defendant engaged in graphic sexual conversations online and transmitted lewd photographs of himself masturbating to the undercover agent. The defendant ultimately appeared at a prearranged meeting at the Bridgewater Sports Arena to engage in sexual activity with the girl and was arrested. On August 13, 1999, defendant pled guilty to 3rd degree endangering the welfare of a child and 3rd degree eluding and on January 21, 2000 was sentenced to three years probation with 364 days in the Somerset County Jail.

State v. Edward Bostonian. Case No. 00-078 / Ind. No. 00-04-00196-I. In winter, 2000, 39 year-old defendant Edward Bostonian met an undercover agent posing as a 13 year-old girl in an online chat room entitled "barely legalf4olderm." The defendant engaged in graphic sexual conversations online and gave the undercover agent detailed instructions on masturbation. The defendant ultimately appeared at a prearranged meeting at the Bridgewater Commons Mall to engage in sexual activity with the girl and was arrested. On June 8, 2000, defendant pled guilty to 3rd degree endangering the welfare of a child and on January 5, 2001 was sentenced to three years probation with 364 days in the Somerset County Jail.

State v. Robert T. Condon. Case No. 00-451 / Ind. No. 00-10-00547-I. In summer, 2000, 57 year-old defendant Robert Condon met an undercover agent posing as a 13 year-old girl in an online chat room. The defendant engaged in graphic sexual conversations online with the agent and gave the undercover agent detailed instructions on masturbation. The defendant ultimately appeared at a prearranged meeting at the Bridgewater Commons Mall to engage in sexual activity with the girl and was arrested. On September, 2003, defendant was tried and convicted of 2nd degree Attempted Sexual Assault and on October 29, 2004, was sentenced to an eight year period of incarceration in New Jersey State Prison, to be served at the Adult Diagnostic & Treatment Center at Avenel.

State v. James Kane. Case No. 00-535 / Ind. No. 00-12-00717-I. In the summer of 2000, defendant James Kane, a twenty-eight year veteran police officer with the Port Authority Police Department, met an undercover officer posing as a 13 year-old girl in an America On Line chat room. Thereafter, defendant Kane engaged in numerous graphic sexual conversations online with the undercover officer using AOL Instant Messenger. Defendant Kane gave the undercover officer detailed instructions on masturbation and sent pornographic images to the undercover officer over the computer. On February 9, 2001, defendant pled guilty to 3rd degree attempting to promote obscene material and on February 8, 2002 was sentenced to probation with 180 days in the Somerset County Jail.

State v. Glen P. Albright. Case No. 03-430 / Acc. No. 03-08-00465-I. In the spring of 2003, 47 year-old defendant Glen Albright (a teacher at Somerset County Vocational and Technical School in Bridgewater, New Jersey) met an undercover detective posing as a 14 year-old girl in an America On-Line chat room. Thereafter, defendant engaged in numerous online conversations with the undercover officer, including instant messages in which the defendant gave the undercover detective specific, detailed instructions on how

to masturbate. Thereafter, defendant was arrested. On August 11, 2003, defendant pled guilty to 3rd degree attempted endangering the welfare of a child and 4th degree endangering the welfare of a child, and on January 2, 2004, was sentenced to non-custodial probation and a $2,500.00 fine.

Child Pornography Cases

State v. Allen May. Case No. 98-620 / Ind. No. 99-03-00176-I. In fall, 1998, police learned that 70 year-old defendant Allen May of Bridgewater, Somerset County, subscribed to an Internet newsgroup dedicated to the dissemination of child pornography. Police investigation resulted in a search of the computer at defendant May's residence. This search revealed hundreds of images of child pornography that defendant May both downloaded from, and posted to, the Internet. On May 15, 2001, defendant May was convicted of 2nd degree and 4th degree endangering the welfare of a child, and on September 7, 2001 was sentenced to five years incarceration in New Jersey State Prison.

State v. James Nafus, Jr. Case No. 03-158 / Ind. No. 03-04-00236-I. In spring, 2003, 25 year-old defendant James Nafus, Jr., a teacher at the Far Hills Country Day School, turned his laptop computer over to a friend because he was having problems with it. Defendant Nafus' friend discovered child pornography on the computer and called he police, who searched the computer and found numerous images of child pornography. On June 6, 2003, defendant pled guilty to 4th degree endangering the welfare of a child and on December 19, 2003 was sentenced to probation and a $1,000 fine.

State v. Christopher Hickman. Case No. 03-203 / Ind. No. 03-06-00323-I. In spring, 2003, 21 year-old defendant Christopher Hickman met and began a sexual relationship with a 14 year-old girl. During the course of this relationship, defendant Hickman engaged in sexual intercourse with the victim and participated in photographing her nude and while engaged in various sexual acts using his computer and web cam. On September 19, 2003, defendant pled guilty to 2nd degree sexual assault, 2nd degree endangering the welfare of a child, 3rd degree possession of psilocybin with intent to distribute, and 3rd degree possession of marijuana with intent to distribute. On January 9, 2004, defendant Hickman was sentenced to four years incarceration in New Jersey State Prison

State v. Robert Mascola, Case No. 05-343 / Ind. No. 05-06-00535-I; State v. Michael Pleban, Case No. 05-344 / Ind. No. 05-06-00543-I, and State v. Mickey Phillips, Case No. 05-345 / Ind. No. 05-06-00536-I. In spring, 2005, the Somerset County Prosecutor's Office received information from Immigration and Customs Enforcement (ICE) that ICE was conducting a large scale child pornography investigation which revealed that several Somerset County residents had purchased child pornography over the Internet. Police contacted these individuals and the resulting investigations revealed that they possessed child pornography on their computers that they obtained via the Internet. All of these individuals were admitted into the PTI program on charges of 4th degree endangering the welfare of a child (possession of child pornography).

Steps Taken by the Somerset County Prosecutor's Office to
Combat the Sexual Exploitation of Children Over the Internet

After recognizing the growing nature of this problem almost ten years ago, when I left the Attorney General's Office to become the Somerset County Prosecutor I took a number of steps to educate and train our police officers, assistant prosecutors, and parents in an effort to combat this problem and protect the children of Somerset County. For example, in 1998 we created a free Internet safety presentation that educates parents and other concerned citizens on the dangers of the Internet and provides guidance for keeping children safe. We also created and distributed free informational brochures for parents and children to provide rules for safe Internet use. In addition, I have sent our assistant prosecutors and detectives for advanced training in investigating and prosecuting these

types of crimes so that we can stay at least one step ahead of the individuals who commit these crimes in the constantly changing area of computer technology and computer crimes. Finally, I created a High Tech Computer Crimes Unit within the Prosecutor's Office to assist in properly investigating these specialized crimes. Through these steps, all of which are described in detail below, I believe the Somerset County Prosecutor's Office provides the citizens of Somerset County with highly trained police officers and detectives to both proactively and reactively investigate these more challenging crimes, assistant prosecutors who are better prepared to prosecute these cases, and the educational awareness to help prevent the sexual exploitation of our children over the Internet.

Internet Safety Presentation for Parents. In 1998, the Somerset County Prosecutor's Office created a free Internet safety program for parents and other concerned citizens entitled "Danger Is Only A "Click" Away: A Parents' Guide to Internet Safety." The program covers Internet dangers, including pornography, child pornography, pedophiles/child exploitation, weapons/explosives, "hate" groups, theft, terroristic threats, narcotics and profiles/blogs, and uses examples from actual Somerset County cases. The program provides parents with advice on how to protect their children, including rules for safe Internet use, warning signs and detailed instructions on how to examine the computer to determine which sites your child has accessed on-line. The program is directed toward parents with minimal computer knowledge and is not suitable for minors due to graphic content. The program lasts approximately one hour with a question-and-answer period to follow. Anyone who attends the program receives a free "Internet Safety Pledge" mouse pad to assist them with teaching their children rules for safe Internet use. Since 1998, the Somerset County Prosecutor's Office presented the program to every school, community and business group that requested it, thereby educating thousands of Somerset County residents about safe Internet usage. (See enclosed copy of PowerPoint presentation, attached as Exhibit A.)

Informational Brochures. In 2001, the Somerset County Prosecutor's Office created two informational brochures entitled "A Parent's Guide to Internet Safety" and "Ten Internet Safety Tips for Kids." The brochures provide parents and children with information on Internet dangers and tips for safe Internet usage, and since 2001 have been disseminated to the public free of charge. (See enclosed brochures, attached as Exhibit B and Exhibit C.)

Advanced Training for Assistant Prosecutors. Several Somerset County Assistant Prosecutors who prosecute these types of cases have received advanced training on prosecuting crimes involving children and the computer. For example, Somerset County Assistant Prosecutors have attended the following courses: (1) Protecting Children Online for Prosecutors, 2005, at the Jimmy Ryce Law Enforcement Training Center in Alexandria, Virginia (sponsored by the National Center for Missing and Exploited Children; (2) High Tech Crimes Investigation Association Training & Conference in Atlantic City, New Jersey, 2002; (3) Law Enforcement and the Internet, Sponsored by the New Jersey Attorney General's Office at Rutgers College, New Brunswick, 2000; (3) Legal Issues in Computer Crimes Prosecutions, Sponsored by the US Secret Service and the High Tech Crimes Investigation Association, at the World Trade Center in New York, New York, 1999, and (4) Investigation and Prosecution of Child Sexual Exploitation, sponsored by the Assistant Prosecutors' Research Institute and the National District Attorneys' Association in Columbia, South Carolina, 1999. In addition, Somerset County Assistant Prosecutors have attended various seminars on high tech crimes and/or computer child pornography issues held during the general annual conference for the Sex Crimes Officers' Association and MAGLOCLEN, as well as classes on legal issues of high tech crime, sponsored by the New Jersey Division of Criminal Justice.

Specialized Training for Detectives. After recognizing the problems for law enforcement presented by the Internet, the Somerset County Prosecutor's Office made a concerted effort to ensure that its Detective Division was prepared to investigate these types of cases. Toward that end, since 1999, the Somerset County Prosecutor's Office has assigned a number of detectives to various other agencies / units that specialize in computer investigations. Specifically, between 1999 and 2001, Detective Andrew Lippitt was assigned to the Federal Bureau of Investigations North East Regional Child Exploitation Task Force (aka, "Innocent Images.") During that time, the Task Force generated more than seventy undercover proactive investigations over the Internet that resulted in arrests of sexual predators. Since that first assignment, the Prosecutor's Office assigned two other detectives to "Innocent Images" - Detective Robert Pascale, from January 2002 to August 2003, and Detective Sergeant Lori Rinaldi, from August 2003 to May 2005. In addition, the Prosecutor's Office sent Detective Lippitt and Detective Pascale to the New Jersey State Police High Tech Crime Unit where they received additional training and experience. Detective Lippitt was there from August 2001 to February 2002, and Detective Pascale was there from August 2003 to May 2004. There, they conducted all types of computer and Internet related investigations, including computer forensic examinations and proactive "traveler" investigations. In addition, Detectives Lippitt and Pascale have attended numerous other courses involving computer investigations.

Creation of the High Tech Computer Crimes Unit. In 1999, the Somerset County Prosecutor's Office created the High Tech Computer Crimes Unit to assist in conducting computer investigations. The unit assists other units with the Prosecutor's Office and other law enforcement agencies in all types of criminal investigations involving computers, including the seizure, search, and forensic examination of computers obtained by law enforcement personnel. In addition, the High Tech Computer Crimes Unit conducts computer related training for law enforcement officers, including a one-day Introduction to Computer Crimes Course at the Somerset County Police Academy that teaches law enforcement personnel to recognize and properly handle a computer crime. The course covers the common types of computer crimes, including sexual predators, child pornography, narcotics, weapons and explosives, and hate groups. Course attendees receive training on how to trace Internet Protocol (IP) addresses found in the header portion of Emails. In addition, the High Tech Computer Crimes Unit has participated with the FBI, ICE, the New Jersey State Police and numerous local agencies in conducting proactive Internet investigations regarding child exploitation and child pornography. The High Tech Computer Crimes Unit is currently in the process of developing and conducting proactive Internet investigations.

Conclusion

While the sexual exploitation of children through the Internet is a serious and growing problem in Somerset County, the Somerset County Prosecutor's Office will continue to take all necessary measures, including the steps described herein, to protect our citizens from individuals looking to victimize our children.

Respectfully submitted,

Wayne J. Forrest
Prosecutor, Somerset County

MR. WHITFIELD. Thank you, Mr. Forrest. And Mr. Banks, you are recognized for 5 minutes.

MR. BANKS. Mr. Chairman Whitfield and Mr. Ferguson and members of the subcommittee, thank you for the opportunity to testify here today. My name is Andre B. Banks and I am a sergeant with over 20 years experience in law enforcement. I work in the Union County Prosecutor's Office in Elizabeth, New Jersey and I am currently assigned to the High Tech Crimes Unit that oversees the Union County High Tech Task Force. The High Tech Task Force investigates all computer and Internet related crimes in Union County.

I obtained my bachelor's degree in Political Science from Kean University and I also have obtained an associate's degree in Liberal Arts. I am a certified instructor for "The Internet and Your Child" and a certified i-Safe instructor, which are both education and training programs designed to teach parents and educators about Internet safety. We have given hundreds of lectures throughout Union County on Internet safety and cyber crime.

The Union County High Tech Task Force was the first New Jersey county to start a High Tech Task Force 6 years ago to investigate child exploitation cases. We work closely with Federal, State, and local authorities in these types of investigations. Several years ago, our office also received a Federal grant to be a satellite office for the Internet Crimes Against Children, ICAC, national task force. We have arrested dozens of Internet predators over the years through the efforts of ICAC.

I am also certified as an Encase Certified Forensic Examiner, EnCe, for conducting detailed computer forensic examinations of seized computers. This becomes very important after arresting an offender and examining his computer for evidence of the crime that was committed. I teach in-service classes to Federal, State, and local officers in Internet crimes at the Union County Police Academy. I am an active member of the High Tech Crime Investigator Association, the New York Secret Service Electronic Crimes Task Force, International Association of Computer Investigative Specialists, and the Institute of Computer Forensic Professionals.

Today, one of the many challenges law enforcement faces is protecting our children from the dangers of the Internet. When I first started investigating Internet crimes back in 1996, it was primarily cases involving distribution of child pornography and e-mail. Today, the predators that troll the Internet have many choices from which to make attempts to lure their victims. There are hundreds of investigations that I could talk about today when it involves the dangers of the Internet. One of the cases that I want to review with you is an investigation that I started a few years ago that involved a 14-year old female named Nicole. I say this is typical because Nicole would come home from school before her mother arrived home from work, between 3:00 p.m. and 5:00 p.m.

and would always log on to AOL's instant messenger program called AIM.

You know about the Internet chatting programs that allow children or Internet users to talk in real time with people anywhere in the world? This teenager used the AIM program to chat with her friends. Some of her friends she had met online and some she knew from school. She met a subject online who said he was also a teenager from New Jersey and he went by the screen name of Lovs2playDoctr. After several weeks of chatting online and making secret phone calls, they became online buddies and Lovs2playDoctr began sending her lewd pictures and talking about sex. This is the grooming process that predators often do to make their victims feel more comfortable talking to them.

One day Nicole's mother came home early from work and saw some disturbing chat conversations and called the Kenilworth Police Department. The PD called my office and I later met with Nicole and her mother and they agreed to allow me to take over Nicole's screen name so I could continue chatting with this subject. I later found out, through a subpoena, that Lovs2playDoctr was actually Michael Jasinski, a 31-year old male from Newark, Delaware, who had a criminal record.

I then went in, an undercover capacity, acting online as if I was Nicole by using her screen name and I continued chatting with this guy, Lovs2playDoctr, until he made plans to meet Nicole for a sexual encounter. I contacted Delaware State Police through ICAC and we eventually arrested Jasinski and executed a search warrant at his house in Newark, Delaware. This case that I just reviewed with you is a scenario that often happens involving our children when they are home alone. They usually feel safe on the Internet using computers and chatting with strangers, even though they know it is not the right thing to do. Jasinski is currently serving 10 years in Delaware State prison.

The second scenario I want to talk about involves the popular website called MySpace. MySpace is a virtual meeting place on the Internet where children and adults can create free accounts to express their creativity and leave journal entries, also called blogs, on each other's pages. This popular website is an awesome technology to many users; however, it can be a nightmare to some people who fall prey to the predators and evildoers who seeks to lure innocent victims.

A recent case in Union County that ended in a tragic death involved a 14-year old female named Judy Cajuste. The victim had a MySpace account filled with many pictures and blog entries from her friends that revealed personal information. The investigation is still ongoing and we believe there may be a link to her MySpace Web page that led to her death. Other MySpace problems occur when parents don't know their children even have a MySpace account. Other MySpace problems occur

also when schoolmates use MySpace to cyberbully other children. I speak to parents all the time during our lectures and also receive phone calls from disturbed parents about harassment that their children are confronted with on MySpace.

This is not only restricted to MySpace. There are many other Web blog Internet sites out there that suspects use to lure and stalk victims as well. I am highlighting MySpace because it is the most popular. One of the things I always tell parents is to become familiar with this technology and see what their children are doing. One incident I like to tell parents about is when a very upset parent called my office complaining about posting bad messages on her daughter's MySpace web page. I advised her the proper way to file a complaint at a local police department, but I also educated her about the website. I asked her if she knew about the security settings that MySpace put in place to block unwanted comments and she didn't know. I then talked her through the steps to block certain users and to prevent blog entries without permission. After showing her and many others how to activate this feature, it often solves the problem.

A good portion of my job at the Union County Prosecutor's Office is community awareness through training classes and lectures on Internet safety. Many parents are clueless when it comes to navigating around on the Information Super Highway. That is why my office has taken an aggressive approach to community awareness by having Saturday classes called the "Internet and Your Child," where parents can come and sit down at a computer terminal and learn what their kids already know about the Internet. We have also started the first "Train the Trainer" program in the State of New Jersey through i-SAFE, where members of our office and the Union County High Tech Task Force teach educators and law enforcement personnel how to give informative lectures to citizens in their communities. I believe this approach we have taken has educated a good portion of the population and has prevented more tragedies from occurring in Union County.

Thank you and I look forward to your questions.

[The prepared statement of Andre Banks. follows:]

PREPARED STATEMENT OF ANDRE BANKS, SERGEANT, OFFICE OF THE PROSECUTOR, UNION COUNTY

Chairman Whitfield and members of the subcommittee, thank you for the opportunity to testify here today. My name is Andre B. Banks and I am a Sergeant with over 20 years experience in law enforcement. I work in the Union County Prosecutor's Office in Elizabeth, NJ and I am currently assigned to the High Tech Crimes unit that oversees the Union County High Tech Task Force. The High Tech Task Force investigates all computer and Internet related crimes in Union County . I obtained my Bachelor of Arts degree in Political Science from Kean University (Union, NJ) and I obtained an Associate degree in Liberal Arts (Walnut, Ca). I am a certified instructor for "The Internet & Your Child" and a certified ISafe instructor, which are both education

and training programs designed to teach parents and educators about Internet safety. We have given hundreds of lectures through out Union County on Internet safety and Cyber Crime. The Union County High Tech Task Force was the first N.J. County to start a High Tech Task Force six years ago to investigate child exploitation cases. We work closely with Federal, State and local authorities in these types of investigations. Several years ago our office also received a Federal grant to be a satellite office for the Internet Crimes Against Children (ICAC) national task force. We have arrested dozens of Internet predators over the years through the work of ICAC. I am also certified as an Encase Certified Forensic Examiner (EnCE) for conducting detailed computer forensic examinations of seized computers. This becomes very important after arresting an offender and examining his computer(s) for evidence of the crime that was committed. I teach in-service classes to Federal, State and Local officers on Internet crimes at the Union County Police Academy. I am an active member of the High Tech Crimes Investigator Association (HTCIA), New York U.S. Secret Service Electronic Crimes Task Force (ECTF), International Association of Computer Investigative Specialists (IACIS) and the Institute of Computer Forensic Professionals (ICFP).

Prior to working in Union County, I worked as a Patrol Officer for the Fullerton Police Dept. in California from 1985 to 1988. In 1988 I relocated to my home state of New Jersey where I was hired by the Morris County Sheriff's Office and was immediately assigned to work at the Special Enforcement Unit of the Morris County Prosecutor's Office as an undercover narcotic agent. I worked in that capacity until Nov. 1995. I was then reassigned to develop the Sheriff's office-wide network database that was used by the four divisions within the Sheriff's office to manage the day to day operations. In July 1996 I was hired by the Morris County Prosecutor's Office as a Detective in the Fraud Unit/Administration Unit. While there, I enforced crimes relating to fraud, theft and started the Morris County computer crime unit. I have attended many police training courses in my career and also other specialized courses in police supervision and computer investigations.

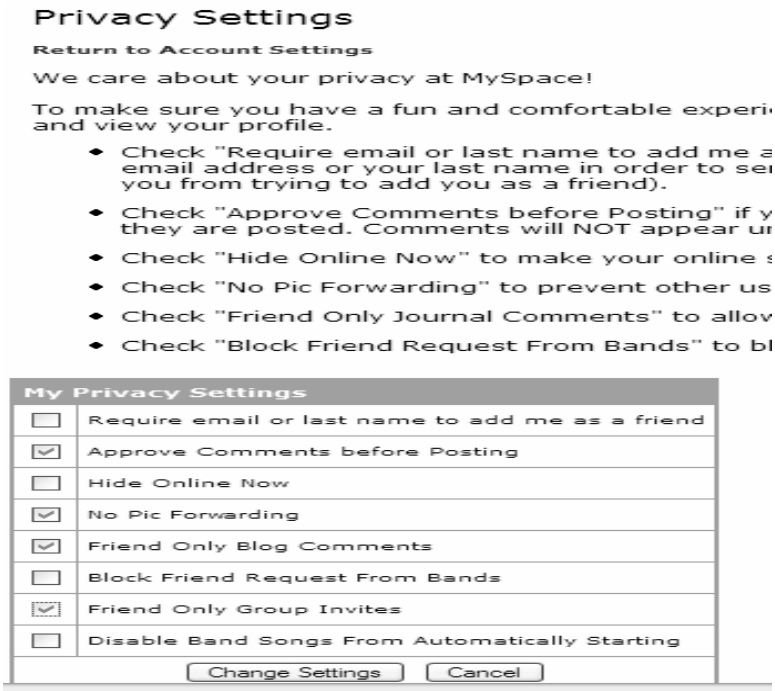
Today, one of the many challenges law enforcement faces is protecting our children from the dangers of the Internet. When I first started investigating Internet Crimes back in 1996 it was primarily hacking cases and distribution of child pornography via email. Today, the predators that troll the Internet have many choices from which to make attempts to lure their victims.

There are hundreds of investigations that I could talk about when it involves the dangers of the Internet. One of the cases that I want to review with you is an investigation that I started a few years ago that involved a typical 14year old female named Nicole. I say this is typical because Nicole would come home from school before her mother arrived home from work between 3pm and 5pm and would always logon to AOL's instant messenger program called AIM. You know about the Internet chatting programs that allow Internet users to talk in real-time with people anywhere in the world? This teenager used the AIM program to chat with her friends. Some of her friends she had met online and some she knew from school. She met a subject online who said he was also a teenager from N.J. and he went by the screen name of *Lovs2playDoctr*. After several weeks of chatting online and making secret phone calls they became online buddies and *Lovs2playDoctr* began sending her lewd pictures and talking about sex. This is the grooming process that predators often do to make their victims feel more comfortable talking to them. One day Nicole's mother came home early and saw some disturbing chat conversations and called the Kenilworth Police Dept. The PD called my office and I later met with Nicole and her mother and they agreed to allow me to take over Nicole's screen name so I could continue chatting with the subject. I later found out through a subpoena that *Lovs2playDoctr* was actually Michael Jasinski, a 31 year old male from Newark, Delaware, who had a criminal record. I then went in an undercover capacity online acting as if I was Nicole, by using her screen name I continued chatting

with *Lovs2playDoctr* until he made plans to meet Nicole for a sexual encounter. I contacted the Delaware State Police through ICAC and we eventually arrested Jasinski and executed a search warrant at his house in Newark, Delaware. This case that I just reviewed with you is a scenario that often happens involving our children when they are home alone. They usually will feel safe on their computers chatting with strangers even though they know it is not the right thing to do. Jasinski is serving 10 years in a Delaware State prison.

Lovs2playDoctr
REAL Picture

The second scenario I want to talk about involves the popular web site called MySpace. MySpace is a virtual meeting place on the Internet where children and adults can create free accounts to express their creativity and leave journal entries, also called blogs, on each others pages. This popular web site is awesome technology to many users, however it can be a nightmare to some people who fall prey to the predators and evil doers who seek to lure innocent victims. A recent case in Union County that ended in a tragic death involved a 14 year old female named Judy Cajuste. The victim had a MySpace account filled with many pictures and blog entries from her friends that revealed personal information. The investigation is still ongoing and we believe there may be a link to her MySpace web page that led to her death. Other MySpace problems occur when parents don't know there children even have a MySpace account or when schoolmates use MySpace to Cyberbully other children. I speak to parents all the time at our lectures and also receive phone calls from disturbed parents about harassment that their children are confronted with on MySpace. This is not only restricted to MySpace.com there are many other webblog Internet sites out there that suspects use to lure and stalk victims as well. I'm highlighting MySpace because it is the most popular. One of the things I always tell parents is to become familiar with this technology and see what their children are doing. One incident I like to tell parents about is when a very upset parent called my office complaining about people posting bad messages on her daughters MySpace web page. I advised her about the proper way to file a complaint at her local police department, but I also educated her about the web site. I asked her if she knew about the security settings that MySpace put into place to block unwanted comments and she didn't know. I then talked her through the steps to block certain users and to prevent blog entries with out permission. After showing her and many others how to activate this feature it often solves the problem.



How Parents can block users and prevent unwanted postings before they happen.

This is the evil side of MySpace

A good portion of my job at the Union County Prosecutor's Office is community awareness through training classes and lectures on Internet safety. Many parents are clueless when it comes to navigating around on the Information Super Highway. That is why my office has taken an aggressive approach to community awareness by having

Saturday classes called "The Internet and Your Child" where parents can come and sit down at a computer terminal and learn what their kids already know about the Internet. We have also started the first "Train the Trainer" program in the state through ISafe, where members of our office and the Union County High Tech Task Force teach educators and law enforcement personnel how to give informative lectures to citizens in their communities. I believe this approach we have taken has educated a good portion of the population and has prevented more tragedies from occurring in Union County.

MR. WHITFIELD. Well, Mr. Banks, thank you and I appreciate the testimony of the entire panel. I am going to ask one question and then I am going to have to participate in a conference call, and so I am going to ask Congressman Ferguson to chair the hearing until I get back.

But, Mr. Forrest, in your testimony, although you didn't talk about it in your oral testimony, but in your written testimony you made reference to a case, a gentleman named James Nafus, Jr., who was a teacher at, I think, Far Hills Country Day School, and he was involved in some pornographic material and so forth. And my recollection was that the testimony, that he paid a fined and was probated and yet he was a teacher. I was wondering if you could just give us an update on that case, what actually happened to Mr. Nafus and so forth.

MR. FORREST. As you said, he was a teacher in probably one of the most exclusive private schools in all of New Jersey, Far Hills Country Day School. He had a personal laptop computer that he was having some problems wtih. He turned it over to someone and asked them to see if they could fix it. And as that person was attempting to fix the laptop, that person noticed child pornography, what he believed to be child pornography. He called the police. They called our computer crimes unit. We went down and got the computer through legal process, got into the computer and discovered that he was in possession of child pornography. In New Jersey, our legislature makes the mere possession of child pornography a fourth degree crime. We have first degree being the highest, fourth the lowest. We don't have felonies and misdemeanors. He pled guilty to a fourth degree crime without a record. There is a legislative presumption for third and fourth degree crimes against incarceration, and he was given a sentence of a probationary term and a thousand dollars fine.

MR. WHITFIELD. And is he teaching now?

MR. FORREST. I do not know that.

MR. WHITFIELD. But there was a misdemeanor charge?

MR. FORREST. Well, we don't have misdemeanors here, but it was a fourth degree, which is the lowest level of crime.

MR. WHITFIELD. Okay.

MR. FORREST. First degree being the highest, fourth being the lowest.

MR. WHITFIELD. Yes. Okay. At this time, I am going to turn it over to Congressman Ferguson and I will be back as soon as I do this call.

MR. FERGUSON. [Presiding] Thank you, Mr. Chairman. Mr. Forrest, just following up on that particular case. Is there any provision in our New Jersey law for multiple offenders of possession or other child pornography? I don't know what the law says, in terms of what our State law says on possession of child pornography. You said that a first-time offender is a fourth degree offense?

MR. FORREST. Well, it depends on what the crime is. And yes, there are provisions in our laws for repeat offenders for all crimes. Again, we have been doing this for about 9 years. We have not yet seen--and I guess that is a good thing and the State Police have more experience and obviously the Feds do than we do in little Somerset County. But we have not seen repeat offenders as of yet in our county. The profile that we have seen again are affluent businessmen, professionals, police officers, school teachers. We have not seen where they have re-offended in our county where we prosecuted them for any crime, let alone a crime involving the Internet or sexual assault or pornography. Now, but to answer your question, yes, if we have a repeat offender, that could enhance the punishment.

MR. FERGUSON. Whether they are a first-time offender or not, are there any provisions with regard to probation or other provisions in the law that, particularly if they are someone who works with children, this fellow is a teacher.

MR. FORREST. Yes.

MR. FERGUSON. Are there any provisions that say they are no longer able to participate in certain environments or jobs? I mean, obviously, a school, somebody would have to have their head examined for him to be hired back after being convicted of a child pornography crime. But are there any provisions in the law which say what someone who is convicted of these crimes is able to do or how--perhaps they have to stay away from children?

MR. FORREST. Yes and no. Clearly the court can impose conditions during the term of probation, although that will end when probation ends. In addition, if you are an employee in a public position, there is a provision for forfeiture for office and a bar from public office forever. That doesn't apply to a private school, which is the case here. David Livingston is our county superintendent of schools. He and I formed a partnership 9 years ago that I thought it was one of the most important partnerships I had ever formed with anyone, because I think where we can fight the war the best from our local level is to educate parents and children, more so parents. Because I know from my own perspective as a parent, 9 years ago my kids knew more about the Internet than I did,

and I found out what I was missing, that is scary. Just last night we went on the Internet, my kids looking for a piece of sporting equipment and we went on one of our local sporting goods Internet stores, and based on the name of this chain of sporting goods store, my son types it in and clicks it, it came back to a pornographic site, and so you have to be very careful on what words you want--what you are going to put into that Internet site. So as far as teachers go, most, obviously, are public school teachers and the penalty was obviously greater, because we do have a disbarment for life if you are convicted. With private school teachers, as in the case with Far Hills Country Day, that wouldn't apply.

MR. FERGUSON. You had mentioned Pat Barnes was here--

MR. FORREST. Yes, Prosecutor Barnes from Hunterdon County.

MR. FERGUSON. --who is a Hunterdon County prosecutor. I just wanted to say hello and recognize him and thank him for being here today and for your work in Hunterdon County.

MR. FORREST. Which, if I may add, is important because, for the same reasons that people said to me, Somerset County, why are you so concerned about that? We are not in one of the biggest counties in the State, like Union County, for example. Well, I don't know if Mr. Banks can tell us how many residents of Union County have two and three and four computers and laptops in their homes, children that is, but we all do. And you go to Far Hills, where they are sending their children who--a very prestigious private school--these children have computers and they have them, unfortunately, in all the wrong places. And so working with David Livingston, the educational component that we put together, I think is one of the most important services we are providing, because parents are coming up to us all the time and say, I never thought of that and you are right, and my kid is kicking and screaming, but we are taking that computer out of their bedroom and putting in the kitchen or the family room or something like that, and something that small is that important.

MR. FERGUSON. Mr. Rodgers, you had actually referenced Rick Fuentes, who is the superintendent of our State Police--

MR. RODGERS. Yes, sir.

MR. FERGUSON. --who I also want to recognize. He is an outstanding superintendent of the State Police we have in New Jersey and we are very fortunate to have him, and I appreciate your work and all the work of the State Police. Could you comment, and could all of you take a moment to comment on this issue of data retention by Internet service providers? A couple of you referenced in it in your oral testimony and some of you have referenced it in your written testimony as well. This is an issue which is coming up now, and if some consensus is not reached on this, it may require legislative action to kind of bridge

this divide. We have law enforcement who are asking for longer, at least 2 years of data retention, and some privacy organizations and ISPs themselves that have some issues with that. Can you comment on that specifically, and would you each take a moment to comment on that?

MR. RODGERS. I am going to speak in general terms, Mr. Congressman.

MR. FERGUSON. Could you just turn to the microphone to face you?

MR. RODGERS. And I am going to turn my time over to my lieutenant, Tony Ritter. It is a problem for us. The business relationship that we maintain with these ISPs, their ability to turn information around to us in a timely fashion, the length of time that they retain that data in order for us to move forward with effective investigations and prosecutions, is critical. And any manner that we could see that memorialized better in legislation to encourage these ISPs to assist us in doing what I believe to be God's work is critical. If I may, I will turn it over to Tony to speak more in depth.

MR. RITTER. Congressman, one of the cases Lieutenant Colonel Rodgers spoke of was the Guardian case, where we arrested 39 individuals. We actually received a hundred and ten referrals. Seventy of those were lost as a result of us not having the ability to retrieve records.

MR. FERGUSON. So there are 70 folks out there who you have a referral to perhaps prosecute, but you couldn't do it because you didn't have the information because it wasn't retained by the ISPs, is that correct?

MR. RITTER. That is correct.

MR. FERGUSON. Okay.

MR. RITTER. And when we ask for you to stand behind CALEA, changes in CALEA, we are not asking for anything more than we get now. We are just asking that it apply to the emerging communications technologies.

MR. FERGUSON. Are there any particular ISPs that you feel are particularly troublesome in dealing with or not as cooperative as others? Is everyone cooperative?

MR. RITTER. We have had issues with all of them on occasion. I don't want to point the finger at any particular one, but we have had, at times, issues with Comcast. I know they have increased their data retention schedule, I believe, to 180 days. I am not sure of the timeframe. We have had issues with AOL. AOL is one of the companies that does not take our legal documents. They have to be rewritten down in Virginia before they are processed. So you know, that adds a little bit of time to the process as well. There are some ISPs, some

of the smaller ones, that don't retain records at all for dynamic IP addressing. So I think everyone, including ourselves, need to step it up.

MR. FORREST. This has to be done a Federal level. Obviously we can't and it has to require Federal legislation nationally. Even that won't solve the problem, but the bottom line is, U.S. Attorney Christie said it, most of these people think they are in the privacy of their own home; they are not going to get caught. Most of them are right. However, when we do catch them, that is what we hear from them. Oh, I didn't think I was doing anything wrong. Or, oh, I never thought you were going to find out. And the reason they think that is because either the ISPs don't keep the data for a long enough period of time. We have a hard time getting it from them. Earlier, somebody talked about following the money. We need cooperation there. So in order to make a meaningful step in fighting this most challenging crime that I have ever had experience with, everybody has to cooperate, and everybody means whoever all the players are today or whoever may join the team later as a player tomorrow. And that has to be mandated by Federal legislation. There is no other way around it. We can't do it in New Jersey and with State legislation, we can't do it, clearly, in Somerset County.

And this is not my area of expertise. All I know is that the obvious is before us. This is going on internationally and people that are doing business in the United States of America have to abide by certain regulations, which now don't exist, and they have to--and that would make our job easier. I think it would prevent people through deterrence, because most of the people that we have arrested in Somerset County, if I were to march them in here now, they are not public enemy number one. They are successful and liked school teachers, a police officer who is well thought of, other professionals. And we may be able to prevent them from doing something that they think they could otherwise do and get away with.

MR. BANKS. I would just like to echo what Lieutenant Ritter said. We have had a lot of cases where I am sending subpoenas out on a daily basis, over a hundred subpoenas in a year, and I would say about 25 to 50 percent of those subpoenas come back nothing because the ISPs don't keep the records. That is a big problem, whether it is--

MR. FERGUSON. How many?

MR. BANKS. I would say about 50 percent of our subpoenas sometimes come back with no records, and mainly because we are dealing with a lot of theft cases, credit card cases, and a lot of victims would wait and call beyond 30 days. So the police officer would take the report and try and act on his investigation, but he would call me requesting a subpoena and we would send it out and the record would be not available.

MR. FERGUSON. You had mentioned you thought 2 years was a minimum of how long you thought ISPs should have to retain data, is that correct?

MR. RITTER. That is correct.

MR. FERGUSON. What is your thought?

MR. BANKS. I would say 2 years would be excellent. That would be good.

MR. FERGUSON. Any other thoughts from the panel?

MR. RITTER. Sir, we find sometimes that leads that we develop extend the length of the investigation, many leads on these computers, and by the time we say, oh, we have got somewhere we need to go, there is nothing to go to.

MR. FERGUSON. In this operation that you had mentioned before, you had 39 folks that you got, 70 who you couldn't get.

MR. RITTER. Couldn't get records on.

MR. FERGUSON. Because you couldn't get records. And you are saying that 50 percent of the subpoenas that you send out on this topic, on this issue, can't be responded to because--

MR. BANKS. Because the record is not available.

MR. FERGUSON. --the records don't exist. That is right?

MR. BANKS. And it is basically a dead end on that investigation. There is nothing else the detective can do.

MR. FERGUSON. Can we talk about ICAC for a little bit? Everyone seems to feel like ICAC is really moving the ball forward, and the cooperation that exists is very positive. The success of the operation is very good, but you have all heard about resources being stretched. Would you each talk about your involvement with the ICAC here in New Jersey? I know you talked about you have the opportunity to lead ICAC at the State Police. Talk about it, if you would, in terms of resources, what you do with the money you get through the ICAC funding, what you would do with more ICAC funding, if you had it, and because you have certain personnel assigned to ICAC, what would they be doing were they not on ICAC, and what is the trade-off? Do you see what I am saying?

MR. RODGERS. Yes, sir. I would like to begin by saying ICAC, to me, really embodies the two principal recommendations in a national intelligence sharing plan and in the 9/11 Report, unity of effort and true intelligence sharing. That is what happens every day with the folks that are assigned to the task force. Would it not be for the funding that is provided to us through ICAC specifically for training, we would not be able to keep our people up to speed with the technology advancements that are out there every day. Mr. Christie made reference to it before with his U.S. attorneys making light of the fact that he has one that has

remained consistent and he moves the others through there, and they do so for good reason. The type of work that is being conducted by these investigators and prosecutors is very difficult, and I will leave it at that. It is not something that I would want to expose our personnel to for an extended period of time; yet the skill sets that they develop through the ICAC training become very difficult to replicate and become invaluable to moving these cases forward. Our ability to continue to get additional folks trained and move them for the couple years to develop the skill sets and then ultimately apply those skill sets and then move them out and bring new people in so that we don't burn them out doing this type of work is critical. That is very difficult to do though, even with the resources that are provided to us today through ICAC. We need more. We need to train more people. We need to move people through here. As Mr. Forrest has said, in his career--and I can certainly second that, I have seen nothing like this, the advancements of this type of criminal activity. It is unprecedented. We need to bring more people into the fold that have these skill sets, and the only way we are going to be able to do that is through ICAC.

MR. FERGUSON. So the ICAC funding you receive goes specifically to what?

MR. RODGERS. To training our people and develop the skill sets to do this type of technical work. It also helps us network with our allied partners and train the community through different educational associations and law enforcement associations.

MR. FERGUSON. And if you had more funding, you would use it for?

MR. RODGERS. Well, we would be able to enlighten that many more officers in our organization and in others to do this type of work. Again, it is unique work, not your typical police work. And it is not something where you can train people up and leave them in there indefinitely. To do so you are really neglecting those individuals personally. And we make it a point to ensure they go through our counseling program on a regular basis. But to simply extend that benefit to them and leave them there in perpetuity would be negligent on our part. So we have to continue to move people through this, and to do so we need continued training and resources.

MR. FERGUSON. Does anyone have anything they want to add to that, because I want to move to a different topic.

MR. RITTER. Yes, sir, if I could, briefly. A large part of the mission is to expand this task force. Everyone acknowledges the need. So what we are trying to do is get task force members to sign up for a minimum of 6 months, preferably a year. We feel it takes a full 2 years of doing this work to even be comfortable, and even then you are not really comfortable. And in those 6 months, we try to get them basic computer

training so they understand the technology of computers. We try to get them basic Internet investigative skills. We try to get them basic forensic skills so they know how to analyze things in the field. That is a lot for 6 months, while they are shoulder to shoulder with our best detectives, going case after case. And then should they leave in 6 months or 12 months, we try and send them with some hardware. If they don't have the resource back in their agency, we help to send them back with the hardware and software tools so that they can continue working as an arm of our task force.

MR. BANKS. If I can just add. We received a $45,000 ICAC grant back in--I believe it was 2001, and that money was very, very helpful to our task force members. When they came to our office for 3 to 4 months of training they received good training. And if the money was continuous after the 2 years, we could have continued with the training and just like Lieutenant Ritter said, send some equipment back with them to their department. And once that funding ended, it was kind of slow getting members to continue coming back and working in the task force.

MR. FERGUSON. I want to move to a different topic. Now, Mr. Forrest, you had talked about, in your testimony, this term "grooming," this process that happens with a potential predator and a potential victim. That is a term we have heard in our hearings. Can you describe a little bit more of what you have seen and what your team has seen in terms of how this "grooming" process takes place? What happens?

MR. FORREST. Actually, he could probably do it better than I. He has probably been "groomed" when he portrays a victim, by some of these pedophiles. You may be better to do that.

MR. FERGUSON. Mr. Banks, would you mind?

MR. BANKS. Sure. The "grooming" process is almost like a text book that these predators read on how to talk to children. First of all, the suspects do their homework. They will go onto AOL's database and they will search the database for people that may interest them, children. So once they find several kids that interest them, they may be 13 or 14 years old, the kids that reveal so much information.

MR. FERGUSON. I am sorry. What database are you talking about?

MR. BANKS. AOL's. AOL has an online database for members to search other members to associate.

MR. FERGUSON. So you can just go in? I have not done that.

MR. BANKS. Yes.

MR. FERGUSON. You can go in and search for other members in AOL's database that they provide to their members?

MR. BANKS. Exactly, yes. If you are an AOL member, you can log on and search--

MR. FERGUSON. And look at other people's profiles?

MR. BANKS. Exactly. So once these predators do their homework, they will find the kids that they want to put on their friends list, their buddies list, and they will start chatting with them. Now, they may start out slow. They will start out--they will find out from the kid's buddy list, from their profile--excuse me--what their interests are. Once they find out what the interests are, they will start chatting with them and talk about those same interests. And they will eventually start to send pictures. They may send pictures of clothed people, and then they will send pictures of some partially removed clothing or they will start talking about sex, and this victim will feel comfortable with talking with this predator, because they are talking about things that their parents don't talk to them about, sex. And they are curious and this intrigues their interest and that is how the grooming process starts, and it ends with a sexual encounter most times.

MR. FERGUSON. Would you talk a little bit more about--we have heard a little bit that there is--these predators are teachers or law enforcement, police officer I think you said. Two things. Is there a description of a typical predator? And also, is there a profile of a typical victim? Is there a certain age group? Is there a certain type of young person who ends up being the victim more often than not, or that is particularly targeted by these predators?

MR. BANKS. I would say that there is no particular profile of the predator. We haven't determined that. There is no profile. A predator could be any background. That is number one. And we have not determined if there is a profile for a predator. The victims, I would say, from conducting these investigations with partners in law enforcement, I would say most victims would be shy children that may not have many friends in school, they are out of the social norm, and they are more subject to having online buddies, because the people at school may not become their friends. So they want to seek friends online, and that is where MySpace comes into play, the social Web portals, and a lot of the online programs.

MR. FORREST. What we have seen, Congressman, in Somerset County is the people that walk into the 7-Elevens and come from other counties, more urban areas, come here in a stolen car and stick up the 7-Eleven, is not the same person that now has a sophisticated computer in their private home, because they don't have a home and they don't have a computer. The profile of the defendants that we have arrested, and I have given to you in the written statement, are people generally in their forties, generally affluent, generally successful, generally married, generally with children, and that is just for us. You know, we are just a microcosm here, and maybe throughout the State, the State Police can

say they have seen something completely different. But that is what we have seen in our county.

And similarly with the victims, we have seen mostly females, although we have had male victims. They are mostly people who do not have their parents looking over their shoulders day and night. They are mostly young men and women who do not have the computer in the kitchen, in the family room, where there is a lot of traffic. There are a lot of children that are home alone. Predators know a good time to speak to them would be between getting out of school and before dinner when the parents get home and they may be home alone. Typically, when we have actually seen the children ourselves, it is generally not the cheerleader on the team or the captain of a team. It is someone, as Detective Banks was saying, that may be a little bit more looking for friendship and that is why they are on a computer, and that is why they are more susceptible to being "groomed" and more susceptible to going to the Bridgewater Mall, the Bridgewater Sports Arena, to meet this person. Like in Wahler's case, who, if I recall correctly, initially told the victim that he was around 14, 15 years old. Then he said, well, I am really 17 years old, and all of this that takes place, takes place. But it turned out that he was in his 40s, maybe like 48, and then sexually assaulted her. So we have seen a group of defendants who fit into general characteristics that I think is telling. Now again, I have no familiarity with what goes elsewhere in the State, but that is what we have seen here.

MR. FERGUSON. I have covered a lot of ground, Mr. Chairman. I yield back.

MR. WHITFIELD. Okay. Thank you, Congressman Ferguson. Mr. Banks, you did mention in your testimony about a young lady named Judy. What was that last name, Cajuste?

MR. BANKS. Yes, sir.

MR. WHITFIELD. And she lived in Union County?

MR. BANKS. Yes, sir.

MR. WHITFIELD. And she was 14 years old?

MR. BANKS. Yes.

MR. WHITFIELD. And she was actually murdered, is that correct?

MR. BANKS. Yes.

MR. WHITFIELD. And is that an ongoing investigation?

MR. BANKS. Yes, it is. I can't reveal too much information about the case. It is ongoing.

MR. WHITFIELD. But she did have a MySpace account?

MR. BANKS. Yes.

MR. WHITFIELD. Okay. Now, you also mentioned and I believe Mr. Rodgers mentioned briefly your efforts to provide some educational opportunities for programs for schools and students, and I was

wondering if you all could elaborate on that just a little bit, and do you work at all with i-MENTOR or WiredSafety, or is that something that you are not really involved in with those programs?

MR. RODGERS. May I defer to Lieutenant Ritter? Tony?

MR. BANKS. The two programs that we are involved with, the first program is the Internet and Your Child. That program was created by Leann Shirey. She is a sergeant at Seattle P.D. She received a Federal grant several years ago and that program is designed to have parents come into a computer lab, sit down behind a terminal, and learn what their kids know about the Internet. It is a 4-day course. It is free. They receive a three-ring binder with a bunch of material, and learn about the in-semester programs, MySpace and what have you. That is the first program and we have been doing that since early--I think it was around 2002 we started that program. The other program is i-SAFE, which you all know about i-SAFE, which is an awesome program geared for law enforcement, educators, and concerned parents to be trained. It is an online training program. It also is geared for detectives or educators to educate people at lecture settings at PTA groups, meetings and things like that.

MR. WHITFIELD. And you do a lot of that?

MR. RITTER. Yes, we do.

MR. WHITFIELD. And Mr. Rodgers, you all--

MR. RODGERS. We have trained over 30,000 around the State of New Jersey in the last number of years, and it is from the different educational associations and law enforcement associations. The specific programs, I would have to defer to Lieutenant Ritter to speak to.

MR. RITTER. My understanding is there are about two million children in the State of New Jersey, so reaching 30,000 is not a lot, although we think it is a lot. The ICAC Task Force does partner with NetSafe and they do endorse i-SAFE, and they both provide a great deal of very positive materials.

MR. WHITFIELD. Well, you don't have any sort of a hotline in the event that some young child feels like that maybe they are talking to someone that is not who they think they are? Do you have any sort of hotline?

MR. RITTER. Hotlines are hard to find on the Internet.

MR. WHITFIELD. Are what?

MR. RITTER. They are hard to find on the Internet.

MR. WHITFIELD. Okay.

MR. RITTER. We do have a 24-hour capability.

MR. WHITFIELD. Right.

MR. RITTER. However, if you have ever searched the Internet and you have come across anything, there isn't a magic button to press to

take you to law enforcement, or even to report it. And many times, if you go to websites and look for online safety materials, it takes a concerted effort to get there.

MR. WHITFIELD. And that would be a useful tool to have, I would think. I know, in Great Britain, they do have a program like that, where you can go to a red button and touch and give the information, but I don't think we have a national program like that in the United States.

MR. RODGERS. If I may, Mr. Chairman? To put in perspective here with cyber tips, we also--our high tech folks do that type of work, and how many did we receive last year, cyber tips? Sixty-five thousand, I believe.

MR. WHITFIELD. Sixty-five thousand.

MR. RODGERS. That is cyber fraud. And as Tony had just testified to, we are the largest game in town and we only have 10 folks assigned full time to doing that. So they are doing both the Internet predator work and also cyber fraud.

MR. WHITFIELD. So everybody needs more funds and more manpower, really, to deal with this.

MR. RODGERS. It is a huge problem.

MR. FORREST. While you were out, Mr. Chairman, I had mentioned to Congressman Ferguson that one of the most important things we do is training for parents and children. In your packet, you were given a total of 80 slides. It is a PowerPoint presentation that we present to our various schools and parent organizations. And this is also on our website. And you were asking about a hotline. We have an Internet hotline on our website and then we also have a toll-free number as well. We have brochures such as this, which is also--and we will give you copies of all of this which we give out to parents, we give out to students, and then we put these in the schools and we also give them the programs for the parents and the students to take home. It is a mouse pad, obviously. And it gives the rules of the Internet. We tell the parents to go over this with the children. And when they are fighting with their kids about moving the computer out of the room they will blame it on us. And we will say, well, the prosecutor's office told us we had to do it, so your parents aren't the mean people, it is the prosecutor's office, which is fine. So it is important to educate the public. We try to do that. We try to make it a priority. We get a number of tips over our Internet line, our website, and we also get a number of tips over our toll-free telephone line as well.

MR. WHITFIELD. Well, I want to thank all of you for the great work that you are doing and the leadership that you are providing, and we genuinely appreciate the insights that you gave us and we look forward

to working with you as we continue our efforts in this arena. So thank you very much.

MR. FERGUSON. Thank you.

MR. RITTER. Thank you.

MR. BANKS. Thank you.

MR. WHITFIELD. At this time, I would like to call up the fourth panel, and that is Mr. David S. Livingston, who is the Superintendent of Schools for Somerset County, New Jersey, and he is going to be accompanied by Mr. Mike Herrera, who is the Vice Principal of the Somerset County Vocational and Technical High School.

MR. FERGUSON. I think there is another--there is more to the panel.

MR. WHITFIELD. Oh, there is more? Okay. I thought we had a separate panel, but we are going to call up some other witnesses to be a part of your panel, Mr. Livingston. I am also going to ask Ms. Parry Aftab, who is the Executive Director of WiredSafety, who is from Irvington-on-Hudson, New York. And then Ms. Shannon Sullivan, who is a Teen Angel with WiredSafety, and also from Irvington-on-Hudson, New York. And then Ms. Samantha Hahn, who is i-MENTOR, i-SAFE America, from here in New Jersey. So if you all would all come up and hopefully, do we have enough room for everybody?

MR. FERGUSON. Sure.

MR. WHITFIELD. And do we have nameplates for everybody?

MR. FERGUSON. I am just getting them out now.

MR. WHITFIELD. He is getting them out. All right. And if you all would remain standing, as you know, we like to take testimony under oath with Oversight and Investigations, and I know some of you have been before our committee before. So if you would raise your right hand?

[Witnesses sworn]

MR. WHITFIELD. Thank you. Well, you are sworn in now and, Mr. Livingston, we will begin with you and we will recognize you for 5 minutes for your opening statement.

STATEMENTS OF DAVID S. LIVINGSTON, SUPERINTENDENT OF SCHOOLS, SOMERSET COUNTY, NEW JERSEY, ACCOMPANIED BY MIKE HERRERA, VICE PRINCIPAL, SOMERSET COUNTY VOCATIONAL AND TECHNICAL HIGH SCHOOL; PARRY AFTAB, EXECUTIVE DIRECTOR, WIREDSAFETY; SHANNON SULLIVAN, TEEN ANGEL, WIREDSAFETY; AND SAMANTHA HAHN, i-MENTOR, i-SAFE AMERICA

MR. LIVINGSTON. Thank you very much, Congressman. I am pleased to be here and present information.

MR. WHITFIELD. And if you all would move the microphone over to Mr. Livingston, I would appreciate that.

MR. LIVINGSTON. Okay. Can you hear me now?

MR. WHITFIELD. Yes, sir.

MR. LIVINGSTON. I work as a representative of the Commissioner of Education in this county, and we have about 55,000 students, 79 schools, and 19 districts, and each has its own chief school administrator or superintendent, business administrator as well curriculum coordinators, and principals. I also work with them on a regular basis. On monthly meetings, we meet and do trainings and so on, and my office gets involved in many things. We are generally doing--all kinds of issues come up that we get involved with. Of course, Internet issues and safety are one of those issues that keep cropping up and have been around for a long time.

In each of our districts there are technology coordinators. It is their job to assure that the hardware and software is up to date, is working, and that servers and systems are secure from misuse or abuse of policy. Each district requires every student to sign a contract, stating that they will not violate school policy and restrict the use of Internet to approved websites. Any violation will result in the loss of access to the Internet. And each student has his own ID number that tracks all use. There is an elaborate software system that blocks sites such as MySpace and Photobucket and all other kinds of sites that they consider obscene or in violation of board policy.

I have also attached to the testimony a copy of a letter that went out from one of our superintendents and it was shared with all the rest who did the same thing, in which they note--the major problem that I hear from them is a lack of monitoring by parents of their minor children's activities on cell phones, personal Web pages, and the Internet at home. They do not indicate there is a problem with pedophiles at the school level. Now that is not a sample of every superintendent, but at the meetings we have talked about this and it has been clear that that is not the major issue that they face at the school level, given the fact that students know that it is being monitored.

As the prosecutor mentioned to you, Prosecutor Forrest, I have been in the county also 9 years, I have been in education 38 years, and we have done a lot of trainings together over various issues, whether it be weapons, harassment, bullying, and one of the trainings that we are going to be doing in the fall with the prosecutor's office is Internet safety. That has cropped up because of what you are hearing today, in an attempt to bring to focus conscious-level thinking what superintendents, principals,

all kinds of technology people and teachers are dealing with and how to deal better with problems of Internet safety at the school level and also in terms of students--and better educate students in terms of Internet safety.

So not only will I be doing Internet safety, but bullying and harassment and other abuses are also going to be covered in this workshop, because there are requirements in New Jersey for bullying policies and implementation of trainings for all teachers. There were also memoranda of agreements that are annually updated and reinforced between law enforcement and school officials that every New Jersey district must implement. These contain agreements and protocols between law enforcement and educators so as to create better understanding of how to deal with an arrest or how to deal with a violation or possibly how to cooperate in apprehending criminal behavior.

In short, the recommendations that in the short time I had to research, were that we make available training lessons on Internet safety protocols for parents and school districts to use with teaching staff. And as I mentioned, we are planning to do that this fall with the prosecutor's office. They are well trained and well equipped, as you heard, and have been working with parents for a number of years on this problem. Also, one of the things that I guess I don't know if you can do anything about, but I hear it over and over again, is to make parents and guardians responsible for monitoring minor children's Web pages and e-mail correspondence in their homes. It is very easy to say; it is not very easy to do. And one of the things that isn't mentioned here but is, unfortunately, in these trainings that do occur, whether it be done by the prosecutor's office or by the school, very few parents turn out for those trainings, and so they are unaware. In many cases you are preaching to the choir of those people that come out to do it. Some districts are doing this on back-to-school nights in an effort to get at the audience, a bigger audience, if they can and they will include it in that setting and that is not a bad idea.

The other thing that I hear a lot about are freedom of speech concerns raised by such groups as the ACLU. And parents having easy access to sites their children may be abusing. Restrictions on access do hamper some police investigations as well. We hear that. The problem of monitoring proxy sites in the school setting is ongoing, also, I am told by technology coordinators. Students use a proxy server such as vtunnel.com and can gain access to sites not picked up or filtered by the district's software. So as a result, technology coordinators nightly are updating their filters with new words, new words that may be very innocuous, that you would never think would lead to an obscene website.

So coordinators and school officials I talk with really have no recommended legislation other than to require districts to have signed contracts between parents, guardians, minors and the school, agreeing not to violate school policy, and such contracts should be routinely collected annually from all students using the school Internet services. And I have attached newspaper articles, also. The headlines talk about "Kids: Site Only As Dangerous As The User," and that is a recent article, May 14, talking about the problems with MySpace; and a second one which is two different people from Howell Township, a rather large district in Mercer County. Tom Letson mentions that students--he says the problem is when kids have access to the Internet without any supervision, you get abuses. And if you are not going to monitor the computer, he says, then don't let youngsters have their own access. Of course the other person mentioned in the article is a technology manager in that district, and he says it all comes back to mom and dad or the guardians. Don't permit the computer to be located in the bedroom. Don't allow pictures to be posted.

So I think, from our standpoint, we are really aggressively going to look at training and what we can do with training in terms of our administrators and teachers and principals using the partnership with the prosecutor's office, because they are much more expert in terms of all of the problems that occur. Thank you.

[The prepared statement of David S. Livingston follows:]

PREPARED STATEMENT OF DAVIS S. LIVINGSTON, SUPERINTENDENT OF SCHOOLS, SOMERSET COUNTY, NEW JERSEY

I work for the state as the representative of the Commissioner of Education in Somerset County. We have 55, 000 students, 79 schools, and 19 districts in Somerset County. Each district has its own administrative staff including a chief school administrator, school business official, curriculum coordinators and principals. There are over 600 school districts in New Jersey.

My role includes daily interactions with school districts, approval of budgets, review of certification of public schools every 7 years. I assure special education mandates and state laws and regulations are carried out. My office reviews grants, e.g. IDEA, NCLB, etc. for accuracy. I meet monthly with all school business officials and superintendents. I also mediate disputes that arise between districts and/or their constituencies.

Technology coordinators are employed by each district. It is their job to assure all hardware/software is up to date, is working and that the servers and systems are secure from any misuse or abuse of policy. Each district requires every student to sign a contract stating that they will not violate school policy restricting use of the internet to

approved websites. Any violation will result in loss of access to the internet. Each student has an ID number that tracks all use. There is elaborate software that blocks sites such as **Myspace.com** and **photobucket.com**.

I have attached a letter to parents from one of our superintendents that I shared with all superintendents in my county. Note that the major problem I hear about from principals and superintendents is the lack of monitoring by parents of their minor children's activities on cell phones, personal web pages and the internet at home. They do not indicate there is a problem with pedophiles at the school level.

We are planning to do training for all superintendents in the fall on internet safety. The plan is to assure that trainers will be provided with information and a plan of action to share with all teachers. They, in turn, will train all students concerning the hazards of personal websites and internet chat pages. Bullying, harassment and other abuses are topics to be covered.

In New Jersey, Memoranda of Agreement between law enforcement and school officials are updated each year and contain agreements concerning investigations and protocols for police related to drugs, weapons and harassment.

In short, the following are recommendations for federal legislation:

- Make available training sessions on internet safety protocols for parents and school districts to use with teaching staff. Our county prosecutor's office now provides training for parents and teachers.

- Make parents/guardians responsible for monitoring minor children's web pages and email correspondence in their homes.
- Address freedom of speech concerns raised by such groups as the ACLU. Give parents/guardians easy access to sites their children may be abusing. Restrictions on access hamper police investigations as well.

Finally, the problem of monitoring proxy sites in the school setting is ongoing. Students use a proxy server site such as **VTunnel.com** and can gain access to sites not picked up or filtered by the district software. Lists of words are updated nightly by the technology coordinator to filter any new sites that are pornographic or outside of district policy. Unfortunately, ordinary words can be used to create illicit websites that are not filtered.

Coordinators and school officials I talked with have no recommended legislation other than to require districts to have signed contracts between parents/guardians, minors and the school agreeing to not violate school policy on the use of the internet. Such contracts are routinely collected annually from all students using the school internet services.

I have attached recent newspaper articles about the issues we raised.

MR. WHITFIELD. Thank you, Mr. Livingston. And Mr. Herrera, I understand that you are not going to give an opening statement, is that correct?

MR. HERRERA. I can if--

MR. WHITFIELD. Okay. And keep in the 5 minutes because we are running out of time.

MR. HERRERA. Okay.

Members of the committee, my name is Mike Herrera, Assistant Principal of Somerset County Vocational and Technical High School and father of three children. I graduated from Seton Hall University through the Seton Worldwide Program in Educational Leadership. Seton Worldwide is an online program that provided me with the opportunity to learn anytime, anywhere. My cohorts included educators from Georgia, New Jersey, Pennsylvania, and Rome, Italy. As a school administrator, I am familiar with the paradigm of removing the walls of the classroom while setting up barriers to protect my students.

I would like to talk about how our district views our role as surrogate parents. Students are provided with a proactive, therapeutic approach to the Internet and bullying and harassment. The Somerset County Vocational High School is fortunate to have a school-based onsite program that includes various community services such as a conflict resolution specialist through Richard Hall Mental Health Community Center, and a school resource officer through the sheriff's departments, and various other community resources. We have taken advantage of the State Police's high-tech crimes unit on Internet safety. We chose to focus on our instructors for the initial presentation. It is my belief and hope that our close-knit faculty can positively influence the behavior and character of our students. It has been my experience that a majority of parents are not spending enough meaningful conversation with their children, as Mr. Rodgers referenced earlier. Most of the information is coming from peer-to-peer or over the social network sites. We hope to combat this problem with members of our close-knit faculty.

Prosecutor Forrest discussed grooming earlier of students in negative terms. The Somerset County Vocational and Technical High School faculty is proactive in identifying students to groom in such areas as confidence, conflict resolution, and encouragement.

MR. WHITFIELD. Thanks so much, Mr. Herrera. And Ms. Aftab, you are recognized for 5 minutes.

MS. AFTAB. Thank you very much, Mr. Chairman, and welcome to the State of New Jersey. I appreciate the opportunity to testify again before the subcommittee and it is nice to do it from home. We were identified as being from Irvington-on-Hudson, that is our legal address for WiredSafety, but we actually operate out of New Jersey. And when I used to earn money as an Internet privacy and security lawyer, I used to be able to afford to live in Hunderdon County. Now I can't, so I live in Bergen, which is an interesting State. I am an Internet privacy and security lawyer. I have dedicated the last almost 10 years of my life to

protecting children online. It started when I saw an image of a three and a half year old being raped; it changed my life. I describe it often as having a branding iron applied to your brain. After I vomited and cried for a while, I ended up selling a very expensive home and emptying my bank accounts and my retirement accounts, thinking that the corporations that used to hire me, Yahoo, AOL, Disney, would happily take our advice for free. I have 11,000 volunteers in WiredSafety. We are all unpaid. We are in 76 countries around the world, but most of my volunteers, the ones I rely on the most to operate are here in New Jersey, because I see them. You will be meeting Shannon again. Shannon is one of our Teen Angels. I have Teen Angels in your district, Mr. Ferguson, but they are on vacation this week, so you have a substitute Teen Angel here.

The problem here in New Jersey is not a new one. The first case that we followed on prosecution here in New Jersey was the Paul Brown case in 1996, where the U.S. Attorney, the Department of Justice prosecuted a man from Ohio who was in his 40s. He weighed about 400 pounds; he was an out-of-work postal worker; he lived in the basement of his ex-wife's house. He had found a young girl from Cedar Grove, New Jersey, which is in Essex County, met her online and promised her special access to celebrities. It was a boy band at the time and actually it was probably NSYNC, and some earlier issue, none of us knew what NSYNC was at that time. But he said he knew this boy band and if she would send him pictures, he would get it to the boy band. She did. He asked for sexier ones and they became sexier and sexier. Her mother, ironically, was a teacher. She was a single parent, which is a classic, classic profile of a typical victim. When she found out who he was, this was turned over and he was prosecuted and went to jail. It was one of the very first cases reported anywhere in the United States; that was 10 years ago, and it started here in New Jersey.

We actually recognized over the years--I have been doing this for a very long time--that an awful lot of the cases come from New Jersey. We are wired. We live in a world where parents have two jobs, either because they are fortunate enough or because they have to. The kids have easy access to superhighways. People can get in and out of the State very easily. These are all things that can lead to trouble. When you had asked previously about a typical profile of a victim, actually there are two profiles. The profile that had been testified to is--the wonderful man from Union County--about the loner is the typical profile we thought existed until 4 years ago. Those are the cases that are reported, and the big problem here is, as we are looking at these issues, we really don't know anything more than what is reported. It is all anecdotal. Even the brilliant work done by National Center for Missing

and Exploited Children, or the ICACs, or Innocent Images. None of us really know. We only know what the kids have reported. So the kids who report are 11 and a half to 15. Now that has aged up a little bit because of social networks. Now it is 11 and a half to 16. They are the loners. They come from dysfunctional homes, although that seems to be most of the households in the United States these days. Often single-family homes or broken homes, even if the parent has remarried. They are wired somewhere at home. They engage in communications, sometimes thinking it is a cute 14-year-old boy, sometimes knowing that they are dealing with an adult. Those are the kids who, when something bad happens, report it.

The other kids surprised us. Four years ago, in May, a young girl named Christina Long was killed. It was the first confirmed death by an Internet sexual predator in the United States. She was from Danbury, Connecticut; she was 13; she was co-captain of the cheerleading squad; she was a National Honor Society member; very dysfunctional family, not a very good family life at all. She was now living with her aunt, who was trying to get things worked out, but she was not classically the victim. People Magazine called and asked me to be the expert on the piece and I said, I don't understand it. We have been talking about the victim being these loners and telling the parents, if your kids aren't the loners, you can relax. And now what have we done wrong? What we found is that those kids who are high-risk, they may also come from a dysfunctional family. But those who are high-risk are drinking too much, taking too many drugs, driving too fast, doing high-risk activities, and Internet sexual predator communications are just one of those high-risk activities, and those kids don't report unless they are killed or kidnapped.

So as we look at all of these issues, it is important that we recognize the important and crucial work that this committee has done. I have to tell you that I have learned as much as I have tried to share. And in New Jersey, here the committee can learn that we have one of the best cyber crime units. The New Jersey State Police is one of the best and one of the first in the world that has done this. They will be recognized in our hearing at First Today with our Wired Cops award. And this committee, and you are hearing this for the first time today, will be receiving our Internet Superheroes award, which will be given to you by Spiderman in the fall, because you have done incredible--

MR. WHITFIELD. Well, we look forward to it. I have never met Spiderman.

MR. FERGUSON. I have never met Spiderman, either.

MS. AFTAB. Well, you will now. And he is a real marvel, Spiderman. But as we look at these issues, we all have to work together.

And I am here in New Jersey and I want everyone in the audience that is going to hear this to remember that. The 201 area code is New Jersey, not Washington. So we are here to help.

[The prepared statement of Parry Aftab follows:]

PREPARED STATEMENT OF PARRY AFTAB, EXECUTIVE DIRECTOR, WIREDSAFETY

SUMMARY

Our children are online. They do their homework, entertain themselves, communicate with each other and us, research things, buy and compare prices online. They need the Internet for their education, their careers and for their future. Of all the risks our children face online, only one is certain. If we deny our children access to these technologies, we have guarantees that they are hurt. All other risks are avoidable through a combination of awareness, supervision and parental control and other technologies. More and more children being lured and stalked by online predators who gather information about them from chatrooms, instant messaging, e-mails, websites and the like and use this information to become close to them.

With our children walking around with Internet access in their backpacks and pocketbooks, we can no longer rely on parents watching whatever they do from a central location computer. Our children need to learn to use the "filter between their ears" and "ThinkB4TheyClick." This requires that we get them involved in framing solutions and educating each other. It also requires that we find new ways of building good cyber-citizenship and helping the kids and parents spot risks in new technologies and protect themselves online.

But we also need to recognize that in most cases our children are putting themselves in harm's way. They are intentionally sharing risky information online in profiles, blogs and on websites. They post their cell numbers on their public away messages when using IM technologies. And even when they are careful about protecting their own privacy, their close friends may expose personal information about them by posting photos and information on their profiles. They are also, in greater and greater numbers meeting people offline that they met online. Family PC Magazine reported that 24% of the teen girls they polled and 16% of the teen boys they polled admitted to meeting Internet strangers in real life. Our children go willingly to offline meetings with these people. They may think they are meeting a cute fourteen year old boy, but find that they are meeting a 47- year old child molester instead. This has to stop.

Smart kids are sharing sexual images online with people they don't know, or e-mailing them to others they have a crush on and hope to entice. And with the newer video-chats and technologies, the predators have moved to luring our kids into posing and engaging in sexually explicit activities.

Yet, the actual statistics are lacking. Everything we know is largely anecdotal. In 1999, the FBI's Innocent Images (charged with investigating crimes against children online) opened 1500 new cases of suspects who were attempting to lure a child into an offline meeting for the purposes of sex. Based upon my estimates, about the same number of cases were opened by state and local law enforcement agencies that year. The same year, approximately 25 million minors used the Internet in the U.S., Now, with more than 75 million young Internet users in the U.S. we don't know if the number of instances have increased, decreased or remain flat, given the growth. The crime reporting forms don't collect information about the use of the Internet is child sexual exploitation crimes, or any other crimes. That has to change.

We also need to recognize the real risks and what is hype. Notwithstanding media reports to the contrary, to my knowledge, law enforcement is not aware of anyone who is using the information children provide online to seek them out offline, by hiding behind a

bush or grabbing them on their way home from school. They currently agree to meetings (even if they don't admit it to the police when things go wrong.) But it's only a matter of time before this happens, since universal access to the Internet means that even violent sexual offenders who are online can use it for their own horrible purposes.

WiredSafety.org operates from the computers of its volunteers, but its offices are maintained in New Jersey. Our programs began here and our deepest roots run here. Sadly, one of the first cases of Internet sexual predators also arose here, with a young victim from Cedar Grove communicating with a 46 year old predator from Ohio. One of the few deaths linked to Internet sexual predators also has occurred in New Jersey. As a lifetime resident of New Jersey and a longtime resident of Oldwick, testifying here today means more than any other hearing I have attended. With a state of children who are wired at home, at school and in their backpacks, it is essential that we deliver education and innovative programs to families and young people themselves. Let's start here.

OPENING STATEMENT

SNAPSHOT OF U.S. MINORS ONLINE, IN NEW JERSEY AND HOW PREDATORS REACH THEM

It is estimated that approximately 75 million minors in the Unites States access the Internet either from home, schools, community centers and libraries or from some newer Internet-capable device. This is up more than ten-fold since 1996, when only 6 million U.S. minors were online. Now our children are using cell phones with Internet and text-capability, interactive gaming devices (such as X-Box Live and Sony Playstation Network) with voice over Internet and live chat features, handheld devices with Bluetooth and other remote-communication technology (such as PSP gaming devices and mobile phones) and social networking profiles (such as MySpace, Facebook, Bebo, YFly and others) where they can advertise their favorite things, where they live and pictures of themselves and their friends to anyone who wants to see them.

Ten years ago, when I first wrote my safety tips telling parents to put the computer in a central location, that made sense. It was a central point, where parents could get involved and supervise their children's interactive communications and surfing activities. Now, where they take their communication technologies with them in their pockets, backpacks, and purses, it is not longer as relevant as it once was. Now, instead of expecting parents to watch everything their children are doing online from the comfort of their familyrooms, or kitchen counter, we have to do more. Now, we have to teach our children to use the "filter between their ears" and exercise good judgment and care when using any interactive device. While teaching parents how to supervise their children online was a challenge (I have written the leading books, worldwide, for parents on Internet safety), teaching children to "ThinkB4uClick" is much harder.

When I was growing up (in the days before electricity and indoor plumbing, when we had to walk up hill, both ways!, in blizzards to get to school), parents used to blame us for not behaving. We were disciplinary problems. Now pediatric neuro-psychologists tell us that preteens and young teens are hardwired, through immature brain development, to be unable to control their impulses at this age. Either way, we recognize that preteens and teens take risks, don't appreciate the consequences of their actions and act before they think. When their audience was their school friends, family and neighbors, the risks were containable. When they act out where 700 million Internet users can see, it takes on a much deeper significance.

Putting Their Heads into the Lion's Mouth

Now, I will share something very controversial. While educators and child psychologists understand this, most parents will be shocked at the suggestion that their

preteens and teens are in control of their safety online and putting themselves at risk, often intentionally. But unless we accept this, and direct our attentions at solutions aimed at this reality, we are all wasting our time. We will focus on the much smaller segments of preteens and teens who are being victimized through not fault of their own - those who are targeted at random. All others need to change their online behaviors. And that's where we need to devote all our attentions.

For this to happen, you need to understand the truth. For years we have told parents and minors not to share too much personal information online. "You can be tracked down in real life," we told them. But, notwithstanding anything to the contrary reported in the media and by some local law enforcement officers, to my knowledge, to this date, no preteen or teen has been sexually-exploited by someone who tracked them down from information they posted online. In each and every case, to my knowledge, to teens and preteens have gone willingly to meet their molester. They may have thought they were meeting someone other than the 46 year old who is posing as a teen, but they knew they didn't know this person in real life. They are willingly agreeing to meet strangers offline.

What does this mean? It means we can do something about this. It means we can educate teens and preteens about the realities of meeting people in real life they only know in cyberspace. It means we can create solutions. It means that this is, at least for the time being, 100% preventable. It means that what we do today will have an immediate impact on the safety of our youth. It means we have to join together and work on things that are effective and abandon those that are not.

But we have to act quickly. When I testified before the U.S. House Of Representatives, Committee On Commerce, Subcommittee On Telecommunications, Trade, And Consumer Protection on October 11, 2000, I cautioned:

> Law enforcement is not aware of anyone who is using the information children provide online to seek them out offline, by hiding behind a bush or grabbing them on their way home from school. But it’s only a matter of time before this happens, since universal access to the Internet means that even violent sexual offenders who are online can use it for their own horrible purposes. (See Testimony of Parry Aftab, Esq. U.S. House Of Representatives, Committee On Commerce, Subcommittee On Telecommunications, Trade, And Consumer Protection on October 11, 2000.)

Luckily, while our young people are sharing much more information online than ever before, to my knowledge, predators aren't using it to hunt down our children offline. They are like vampires. They need to be invited in. Sadly, our teens and preteens are too often doing just that. They are inviting them to offline meetings, phone calls and videochats. But, as an expert in cyberrisk management, I can tell you that this is good news. Because we have a single point of risk - our children, preteens and teens. If we stop their risky and unsafe behaviors, and teach them when to reach out for help, we can manage this risk. We can keep our children safe.

Our children are mainly at risk because of their own actions. Some are intentional. Others are inadvertent. They may willingly engage in communications with people they don't know in real life "RL," agree to meet them offline or send them sexually-provocative images or perform sex acts on webcams they share with people they encounter online. They cyberbully each other by advertising their victims for sexual services, posting real or manufactured sexually explicit images of them online or by passing online rumors able their sexual preferences or activities.

Preteens and Teens at Risk: Most of the high risk preteens and teens fall into three categories: those who are naive and looking for love and affection (typically the "loners" and "shy" preteens and teens), those who already engage in other high risks activities, such as drug and alcohol abuse, driving too fast or doing risky things for the thrill of it (often the student leaders, athletes, cheerleaders and very competitive teens, the risks takers and thrill seekers looking to let off steam or impress their peers) and those who don't realize that what they do online is real, the ones who are looking to appear older,

cooler, more fun and more popular (most of the teens and especially preteens fall into this category at least once). Sadly, most of our preteens and teens fit one of these categories. Sadder still is the fact that in recent years we have learned that most preteens and teens are potential victims.

Naive, loners and socially-shy preteens and teens: Some believe that they are communicating with a cute 14 year old boy, who they later discover isn't cute, isn't fourteen and isn't a boy. Most of the reported cases fall into this category, and until the death of Christina Long four years ago this May, experts all believed that *all* victims fell into this category. They are conned, and easy to spot online. Predators can seek them out, and find their vulnerabilities. They are groomed with care, and often fall in love with their molesters. Sadly, when the molestation finally occurs, not only are their bodies broken, their hearts and trust are too.

They need to understand how the predators work online. Too often they tell me that they can "tell" how old someone is online. They can't. No one can. Many predators spend years cultivating the right tone and language to look like a fellow teen online.

These preteens and teens are sitting ducks. While they may have learned not to fall for the "help me find my puppy" ploy offline, they need to learn how that same ploy (appeal for assistance) works online. They need to know how to spot the risks and the predators, when online everyone can look like a cute 14 year old boy. They need to learn that romance shouldn't occur only in cyberspace, and that parents can get involved to help them meet their soul-mate, assuming they really are. So, if they aren't, and turn out to be a 46 year old child molester, they can come home safely and help put that molester behind bars where they deserve.

Risk-takers, Thrill-seeking preteens and teens: Some preteens and teens (mainly teens) are looking for the thrills and challenge of engaging in a relationship (or at least prolonged communication) with an adult. They "play games" with the adult, and are intentionally extra sexually-provocative. They think they are smart enough to do this without getting hurt. They see this as a game, without realizing the consequences of their actions. And crossing the sexual line isn't as frightening online as it would be in real life. The problem is that the consequences are not as apparent, the realities not as immediate. They take risks. And they think they can handle them. (They don't often understand the consequences, though.) They often willingly engage in sexual communications with men they know are adults. That's part of the thrill. They are also often willing to engage in sexual activities with the adult, but don't realize what that can mean when things go very wrong. We rarely hear about these kinds of victims, because they never report it when things go wrong. They feel as though they "asked for it," or are to blame. When we hear of these cases, it's because they are killed or kidnapped. (Christina Long was in this category. She was the first confirmed murder victim of an Internet sexual predator in the U.S. and died four years ago this May.)

Friends are the answer here. If we can get friends too help watch out for each other, it is less likely that they will meet adults in real life, or if they do, got alone. Also, finding cool spokespeople, like Nick Lachey, to explain that it isn't cool to be stupid and campaigns such as our "Don't Be Stupid" help. So do real life stories from victims themselves about how they got caught and advice from the trenches. Kateisplace.org has sections specifically directed at this type of victim. And Teen People is an important partner of ours in spreading the word.

Not really a drunken slut, just playing one online: We've all been reading about this new trend in the news (often with me as the expert). Good, respectful, otherwise well-mannered preteens and teens acting out in cyberspace. In profiles, blogs, on social networking sites and their away messages on IM, on their websites and interactive gaming bios, they act out. They pose in their bras, or worse. They simulate sexual activities (and in some cases post images of actual sexual activities). They pretend to be

someone or something other than what they really are. And this alter-ego may be a sexually promiscuous teen "up for anything."

They don't think it is cool to tell others they were home coloring with their five year old niece last weekend. Instead they claim to have snuck out after everyone was asleep to get drunk at a wild party. To them it isn't real. They lie. They pose. They do thing online they would never dream of doing in RL. They aren't really drunken sluts - they are just playing one online. (Shannon, one of our award-winning Teenangels, will share insight into why teens and preteens are doing this, during her testimony today.)

The Anatomy of a Cyberpredator:

There have been many cases recently where pedophiles and other adults have lured children into offline meetings and molested them. Luckily, there are even more cases when such attempts to lure a child have brought about the attention of law-enforcement groups. I debated whether I should discuss any of these cases, because I did not want to sensationalize them. But if explaining the methods used by offenders might make parents more aware, and their children safer, it's worth it.

Cyberpredators, just like their offline counterparts, usually aren't the scary, hairy monsters in trench coats we imagine standing on a dark street corner. Many are the kind of person you would be inviting to your home as a guest, and often have. They are pediatricians, teachers, lawyers, clergy, vice cops, welfare workers, journalists, Boy Scout leaders, baseball coaches, scientists, etc. They are almost always men. (Sometimes women are accomplices, but rarely are women the molesters.) They are often articulate and well-educated. They come in all shapes, sizes, and colors, and they can be very rich or out of work. But they have one thing in common: they want your child.

Most of us are sickened at the thought of an adult having sexual relations with a child, but to be able to protect our children, we must get into the mind of the predator. First of all, predators often don't see themselves as predators. They see themselves as loving partners with the children they molest. To them this isn't rape, it's a seduction. And, as with any seduction, it's a slow and painstaking process. (Predators have been known to wait more than two years, collecting data on a particular child, before striking.) That's what makes them hard to detect. They don't appear to your child to be dangerous.

An FBI agent who shared a panel with me recently said it best: "Before the Internet, these people had to get physically close to your children. They had to lurk near schoolyards, or playgrounds. Kids would see them. Adults would see them. It was a dangerous situation to be in for them, because everyone would notice an adult male lurking around children. They often had to take jobs and volunteer positions that allowed them to work with children in a position of trust in order to reach their victims. Now, however, the personal risks the pedophiles had to expose themselves to in order to be around children are gone. Now they can be 'one of the kids' and hang out with your kids online without exposing themselves. As long as they don't say or do something in the public room that makes them stand out, they can stay there forever, taking notes."

And, many of them do. They have been known to create large databases on children. They track the children's likes and dislikes. They track information such as whose parents are divorced, who doesn't like their father's new girlfriend or their mother's boyfriend, or who likes computer games or a particular rock group. Kids often share personal information about their lives in chatrooms or on profiles. This is one reason why they shouldn't. The more the predator knows about your child, the more easily they can "groom" them or appear to be their soulmate.

Some cyberpredators (known as "travelers" to law enforcement) seek out the good kids, the smart ones, the ones who are not street-smart and are from sheltered suburban or rural families. Many of our children match that profile perfectly. Others, however, target (or are targeted by) popular, super achiever, risk preferring teens. It took the death of a young teen from Connecticut, Christina Long, before we realized that many of the

incidents involved teens who did not fit the loner profile. What we learned was that these kids never report any attacks or exploitation. The only time we hear of these cases is when the teen is kidnapped or killed.

So who is a typical victim of an Internet sexual predator? Anyone between 11-1/2 and 15. All are vulnerable.

It Doesn't Take Torture for Them to Spill Their Guts

Here's a mock chatroom discussion that my law-enforcement friends and I agree is pretty realistic. Imagine a predatorial pedophile sitting and taking notes on this child, and using this information to lure them later. Would your child fall for this? Most, unfortunately, would. This one is more typical of a boy victim and predator communication than a girl victim communication.

> Child: I hate my mom! I know it's her fault that my parents are getting divorced.
> Predator: I know. My parents are getting divorced, too.
> Child: We never have any money anymore, either. Every time I need something, she says the same thing: "We can't afford it." When my parents were together, I could buy things. Now I can't.
> Predator: Me too. I hate that!
> Child: I waited for six months for the new computer game to come out. My mom promised to buy it for me when it came out. She promised! Now it's out. Can I buy it? Nope. "We don't have enough money!" I hate my mom!
> Predator: Oh! I'm so sorry! I got it! I have this really kewl uncle who buys me things all the time. He's really rich.
> Child: You're sooooo lucky. I wish I had a rich and kewl uncle.
> Predator: Hey! I got an idea! I'll ask my uncle if he'll buy you one too....I told you he's really kewl. I bet he'd say yes.
> Child: Really!? Thanks!!
> Predator: BRB [cybertalk for "be right back"]... I'll go and call him.
> - - -
> Predator: Guess what? He said okay. He's gonna buy you the game!
> Child: Wow, really? Thanks. I can't believe it!!!
> Predator: Where do you live?
> Child: I live in NJ. What about you?
> Predator: I live in New York. So does my uncle. New Jersey isn't far.
> Child: Great!
> Predator: Is there a mall near you? We can meet there.
> Child: Okay. I live near the GSP Mall.
> Predator: I've heard of that. No prob. What about Saturday?
> Child: Kewl.
> Predator: We can go to McDonald's too if you want. We'll meet you there at noon.
> Child: Okay. Where?
> Predator: In front of the computer game store. Oh! My uncle's name is George. He's really kewl.
> Child: Great... thanks, I really appreciate it. You're so lucky to have a rich and kewl uncle.

Saturday arrives, and the child goes to the mall and meets an adult outside the computer game store. He identifies himself as "Uncle George" and explains that his nephew is already at the McDonald's waiting for them. The child is uncomfortable, but the uncle walks into the store and buys the $100 game. He comes out and hands it to the child, who is immediately neutralized and delighted. Stranger-danger warnings are not applicable. This isn't a stranger—he's "Uncle George," and if any proof was needed, the

computer game is it. He gets into Uncle George's car without hesitation to meet his friend at McDonald's. The rest is reported on the 6 o'clock news.

It's disgusting. It makes us sick to our stomachs, but it happens. Not very often, but often enough that you need to be forewarned. (Several thousand cyberpredator cases are opened each year by law enforcement agents in the United States.) But no matter how often it happens, even once is too often. Knowing how they operate and the tricks of the trade will help us teach our child how to avoid being victimized. Each case differs, but the predators tend to use the same general tactics. Aside from the "bait and switch" scam discussed above, they often attempt to seduce a child. They want the child to "want" them.

The Script—How They Operate Online

They begin by striking up a conversation with the child, trying to create a relationship of trust and friendship. They often masquerade as another child or teenager, typically of the opposite sex, unless the child has indicated homosexual interests. (The child may or may not know the "seducer's" real age by the time they meet face-to-face.) Phone calls usually start at this point. Sometimes gifts are sent to the child as well, which may include a Polaroid camera and film. Once they have broken down barriers of caution, they begin introducing sexual topics gradually, often with the use of child pornography to give the child the impression that other children are regularly involved in sexual activities.

Then they begin to approach the child's own sexuality and curiosity, by asking questions and giving them "assignments," like wearing special underwear, sending sexually suggestive photos of themselves to the pedophile, or performing certain sexual acts. These assignments eventually broaden to the exchange of sexually explicit photographs (using the Polaroid, cell phone camera or digital camera) or videos of the child. Finally, the pedophile attempts to arrange a face-to-face meeting. (He may also have divulged his true age or an age closer to his actual age at this point.)

Why It Works

All the lectures we have given our children from the time they are very young about not talking to strangers aren't applicable online, where everyone is a stranger. A large part of the fun online is talking to people you've never met. In addition, our children's stranger-danger defenses are not triggered when other kids are involved. The warnings apply only to adult strangers, not to other children.

If any of us walked up to a child in a playground and tried to strike up a conversation, they would ignore us and probably run away. But if an unknown eleven-year-old came up to another eleven-year-old in the same playground, they'd be playing in ten seconds flat! That's how the pedophiles get in under our kids' stranger-danger radar—they pretend to be other kids. And children often believe what they read and hear. They "know" things about the predator because they believe what he told them. They also believe what they read about him in his "staged" profile, which supports what he told them. So it's not just true, it's confirmed.

There are many stages at which the pedophile can be thwarted by an observant parent. In addition, children with healthy friendships and a strong, open, and trusting relationship with their parents are less likely to fall victim to pedophiles online. Pedophiles typically prey on a child's loneliness. They feed the child's complaints about her home life—creating an "us-versus-them" atmosphere. "Your mom is so mean to you! I don't know why she won't let you _____." (Fill in the blank with whatever we try and limit: makeup, malls, concerts, etc.)

This atmosphere does two things: It creates a distance between the child and her parents, at the same time bringing the child into a special secret alliance with the

pedophile. (You should know that boys are almost as often the victims of Internet sexual exploitation as girls are, but they report it less frequently.)

I have followed many cases over the last few years. In my role as WiredSafety executive director, I've also been responsible for reporting several of these to law enforcement and for helping many families through the pain of prosecution. Sometimes we just help the families survive what the molestation has done to them. (The child isn't the only victim—entire families are torn apart in the aftermath of a molestation.) Parents feel guilty for not having protected their child, siblings don't know how to treat their fellow sibling—the pain can continue for a lifetime, and even more. And, in addition to being hurt physically, the young victim's heart is broken by the betrayal of trust.

Anatomy of a Real and Early Case

One case I reviewed many years ago involved a New Jersey teenager and an Ohio adult predator. It was one of the earliest reported cases of cyber-predatorial conduct, discovered in 1996. Luckily, the liaison was discovered before the girl met the man face-to-face. But it had gone on for a year and a half before being discovered by the girl's mother. As you read the details, think about what could have been done to discover the situation earlier and how you can use these precautions to protect your children.

Paul Brown, Jr., an Ohio resident, was forty-six years old. He was also unemployed, weighed over four hundred pounds, and lived in a basement. He had accounts with several ISPs. Mary (a hypothetical name for the young girl involved) was twelve when her mother, a schoolteacher, bought her a computer, reportedly because Mary was having problems making friends. When she got online, Mary posted a message on an online service, in the spring of 1995, looking for a pen pal. In her message she described herself as a teenage girl. Paul Brown, Jr,. responded to the message, using his real name (something they often do, surprisingly) but identifying himself as a fifteen-year-old boy.

Brown and Mary maintained an e-mail and telephone relationship for several months. As the relationship became more involved, they began writing letters, and Mary sent Brown a photograph. He told her that he was living at home with his mother and was hoping to find a girlfriend. In early August, Brown asked Mary for a "favor." "If I sent you a roll of film, could you get one of your friends to take pictures of you in different outfits and maybe hairstyles? Makeup if you use any, and different poses. Some sexy, if possible. Please. Baby for me. Thanx. You're the best. Love Ya."

Mary complied. For the next eight months, they continued to converse and correspond, and Mary sent additional photos. Brown encouraged her with juvenile antics, such as using stickers in his letters to her saying things like "Getting better all the time!" In May 1996, Brown sent Mary a special love note. "Saying I love you... seems to be an understatement. At the age of 14 you have captured my heart and made it sing... I love everything about you…."

Shortly thereafter, Brown confessed to being in his twenties. He also suggested that Mary videotape herself in sexually provocative poses. She did. After Brown had reviewed her videotape, he returned it to her with instructions to redo the tape and include views of her genitalia and breasts. He later admitted to being divorced and in his thirties. He reportedly also sent her small gifts from time to time.

A few months later, in response to Brown's promise to pass copies of the tape to four members of a rock band Mary admired, she sent additional videotapes to Brown. (Brown told Mary that he knew the band members very well.) Each tape sent to Brown was designated for a different member of the band and contained sexually explicit conduct. Brown apparently had also sent her his size 48 underwear. When her mother discovered the underwear, the authorities were notified. Tracing Brown through phone records, special agents of the FBI in Cleveland seized the videotapes and photos of Mary and of more than ten other teenage girls from across the country.

Mary was fourteen when this was all discovered. Brown pled guilty to enticing a minor to produce sexually explicit photos and videos and was sentenced to a little less than five years in prison (the maximum penalty for a first offense). In a written statement to Brown following all of this, Mary said, "I trusted you. I thought you were my friend."

There are several things that stand out in this case. One, interstate phone calls were made by Mary. Parents should always be reviewing long-distance bills for suspicious calls. Two, Mary was lonely. These kinds of children are often the most vulnerable; a parent should be involved in their online friendships, and monitor their online lives. And, three, as hard as it is to know what our kids are doing when we're not around, especially if you are a single parent, a year and a half is a long time for a relationship to be going on undiscovered. You should spend time learning who your children's friends are, online and off. But Monday-morning quarterbacking is always easier than playing the game in real time. We may look at the situation and say that could never happen to one of our kids. However, there but for the grace of God go all of us....

Knowing your child is lonely and has problems making friends is the first sign that the child may fall prey to a pedophile or cyber- predator. Predators can spot lonely children. They can also spot kids who are new online and may not yet know all the rules. Most teens, when surveyed, admit to having been propositioned online. But what may be obvious to a cyberstreetsmart kid may not be so obvious to a child not yet familiar with cyberspace. Pedophiles befriend these kids and patiently build trust and a relationship—looking toward the day when they can meet face-to-face.

Encourage your children to make online friends, but learning about their online friends is an important way to avoid these secret relationships. Education is important in avoiding this danger, too. (Had Mary been forewarned about how pedophiles operate online, she may have been more attentive to how old Brown sounded on the phone, and been more aware of his classic tactics.) So is control over incoming and outgoing information when younger children are involved, using technology blockers, monitors, and filters. These kinds of situations can be avoided if you plan ahead, educate and communicate with your children, and keep your eyes open.

Getting in Under Your Radar:

Even when parents are watching, bad things can happen.

I included the Paul Brown case in my first book, A Parents' Guide to the Internet. (He was sentenced in 1997, when I wrote the book.) I included it because it was a good example of how cyberpredators typically operate, and suggested that if the mother had been a bit more attentive, it might have been discovered earlier. I was right about how cyberpredators operate. I was wrong about how being attentive might have avoided the sexual exploitation. It takes more. It takes both an attentive parent and a teenager who has been taught how these pedophiles operate online.

In November 1998, I met a mother who did everything right. She was attentive and inquisitive about her daughter's online relationships. She asked the right questions. She had a good relationship with her daughter, and yet Charles Hatch, a child molester from Utah, got in under everyone's radar and sexually exploited her thirteen-year-old daughter.

Jennifer (not her real name) was eleven and a half when she first met "Charlie" online. She thought he was a few years older, and was intrigued about befriending a slightly older teenage boy. Jennifer was an honors student and had already been taking advanced college courses while still in middle school. She lived in a loving and warm household with her mother and father. She also had siblings and half siblings from her father's previous marriage. They were all close.

Jennifer's mother, Sharry (also not her real name), talked to Jennifer about her online friend, Charlie. She insisted on talking to Charlie himself, by phone, once he and Jennifer had started calling each other. He passed the phone call test, and Sharry was convinced that he really was the teenage boy he professed to be. Either he had

manipulated his voice to sound younger or he had a younger person make the call. Charlie even called and spoke to Jennifer's brothers, talking about when he would be their brother-in-law someday, after he and Jennifer were married. He pleaded with Jennifer to come and visit him in Utah. Sharry invited him to visit them instead. But Charlie always had a reason he couldn't come.

As things progressed, Sharry insisted on talking to Charlie's mother. He first avoided it by saying she was sick, later that her sickness had become cancer, and that eventually she died from the cancer. The family fell for this, hook, line, and sinker. Most caring families would. Although the "relationship" progressed for almost two years, it remained relatively tame. Charlie was romantic rather than predatorial, and he sent her expensive gifts, including a Polaroid camera. (Remember the Polaroid camera Paul Brown sent?)

Jennifer was inexperienced with boys and dating, and Charlie seemed to know not to push her too fast. But about a year and a half after they met online, Charlie sent her sexually explicit photos of himself from the neck down. She became very uncomfortable and pulled back. But several tragedies occurred around the same time, which made Jennifer easier prey. Her father was hospitalized with a serious illness, and her sixteen-year-old half brother died of a brain hemorrhage.

Charlie, like all good predators, knew when to strike. He told Jennifer that she owed him sexually explicit photos of herself, since he had sent those of himself. When she refused, he told her that she would be left alone, since her family was dying or would die—and he threatened to leave her. Reluctantly, after fighting against it as hard as she could, she acquiesced and sent him sexually explicit photos of herself.

When Sharry was cleaning Jennifer's room, she discovered a letter in which Charlie had set forth the sexual poses he wanted Jennifer to photograph. Sharry sent him a letter, confronting him. She said that he didn't sound like a teenager in the letter. She told him that if he ever contacted her daughter again, she would inform the police. He never replied, and Jennifer was not permitted to use the Internet for months.

One day, just when Jennifer and Sharry thought that the whole episode was past them, the phone rang. It was a detective from Utah, who informed Sharry that Jennifer's photos had been discovered in Hatch's day planner by a coworker. He wasn't sixteen—he was thirty-six. He was a former teacher who had been dismissed by the school after having been accused by a student of sexual abuse. (The school hadn't taken any other action.) He was currently employed by the welfare office in Utah, and was married with children and step-children.

Six months later, Charles Hatch was convicted of sexual exploitation in a Utah federal court. He began his six-and-a-half year sentence in early June 1999. As a condition of his plea, he will not be permitted to use the Internet. This mother has become a dear friend of mine, after seeking WiredSafety' help in getting through this. She was the first parent to speak out publicly about her child being targeted by a sexual predator online.

Unfortunately, the predators are willing to try many different ploys until one finally works.

Using Celebrity's Names

I was having lunch in Los Angeles with one of my girlfriends when Nick Lachey walked into the restaurant. She pointed him out to me and I immediately grabbed my business card and approached his table (to the utter embarrassment of my friend). I introduced myself and told him I needed his help. I explained that predators were using his name and the name of other celebrities to lure kids into meetings and unsafe activities. They find teens who post their favorite celebrities on their profiles, websites or other online communications. Then they create a profile claiming to be a close personal friend of that celebrity. They offer to forward a pic of the teen to the celebrity, and seek sexier

and sexier pics as time goes on, ultimately ending with an offer to introduce the teen to their favorite celebrity in real life. Years ago, Justin Timberlake was the most popular of these celebrity lures. Nick is now. He listened intently and turned white when he realized people where using his name to hurt his young fans. He offered his help.

When I left his table, he has agreed to do a public service announcement to help teens understand that is anyone claims to be a close personal friend of a celebrity, they aren't. Or won't be for long. I was very excited, but not as excited as I was two weeks later when someone from Nick's office called asking me to help them create a safer teen-only social networking site called YFly.com. I agreed and YFly.com became a reality with the financial assistance of Tom Petters (and the Petters Group), and the creativity and energy of its founders, Drew Levin and Daniel Perkins. I joined the team to set up a safer network and create the most advanced educational and awareness content online, just for teen users. The young users can click on "Report the Creep" if they suspect someone is an adult posing as a teen.

It's a beginning. Finding safer technologies and services is part of the solution. So is awareness using teenspeak.

Delivering Teen-Designed Messages Using their Media

For the first time, other than at our summit on social networking last month, we are showing our "You Never Know..." animation series. Designed by teens for teens and preteens they help bring home the point that you never know who is pretending to be that cute 14-yr old boy or girl. These tiny animations are designed to be cell phone friendly and easily sent from preteens and teens to each other. The more we can get them to think about who they might be communicating with, the safer they will be.

Shannon, one of our Teenangels is 14 years old. She was selected by Teen People as one of the twenty teens who will make a difference. She has gone them one better...she is already making a difference. It is with pride that I introduce Shannon Sullivan, one of my Teenangels.

APPENDIXES:

Appendix 1: Overview of WiredSafety.org

WiredSafety.org is a 501(c) (3) charity and the largest and oldest online safety, education, and help group in the world. It consists of thousands of volunteers from more than 76 countries around the world, all working online with the mission of promoting a safer and more responsible Internet and wireless experience for everyone.

Originating in 1995 as a group of volunteers rating websites, it now provides one-to-one help, extensive information, and education to cyberspace users of all ages and members of the Internet industry on a myriad of Internet and interactive technology safety issues. These services are offered through a worldwide organization comprised entirely of volunteers who administer specialized websites and programs. WiredSafety.org volunteers range in age from 18 to 80 and run the gamut from TV personalities, teachers, law enforcement officers, PhD's, writers and librarians to stay-at-home moms, retired persons, and students. WiredSafety.org's founder and Executive Director, cyberlawyer Parry Aftab, is also an unpaid volunteer. With the exception of its TeenAngels, outreach and speaking programs, all work and help is provided online and free of charge.

WiredSafety.org's work falls into four major areas, all designed to help promote a safer and more responsible digital experience for everyone:

- **Assistance** for victims of cyberabuse and harassment and others who need help online, including parents, teens and educators.
- **Advice, Training and Help** for law enforcement worldwide on preventing, spotting and investigating cybercrimes and for members of the Internet and interactive digital industries in designing safer technologies and adopting and implementing best practices.
- **Education** for children, parents, communities, law enforcement, abuse and customer help staff within the Internet industry and professional development for educators.
- **Information and Awareness** on all aspects of online safety, privacy, responsible use and security wired, wireless and as new technologies are developed.

Our target audiences include:

- Parents, grandparents and caregivers (including aunts, uncles and older siblings);
- Pre-reader lap-surfers, kids, preteens, teens and college students;
- Members of the Internet, wireless and interactive technology industries;
- Law enforcement, community policing agencies and school resource officers, legislators, the judicial community and regulatory agencies; and
- Schools and other educational institutions.

Originally formed in 1995 (under another name) to provide help and protection for Internet users of all ages, in recent years, Wiredsafety.org's work has increasingly focused on the safety and good cybercitizenship of children, tweens, and teens. It serves as the umbrella organization for TeenAngels.org, WiredKids.org, WiredCops.org and

WiredTeens.org. WiredSafety.org is dedicated to protecting children in cyberspace from cybercrimes and abuse, including from each other. This involves protecting them from cyberbullying, hacking, sexual harassment and identity (ID) theft. It also includes protecting children everywhere from Internet-related sexual exploitation. WiredSafety.org helps protect them from risks posed by adults, by each other and more recently from themselves, as their reputations and future college and job opportunities are impacted by what they post on their MySpace and other profiles. The package of programs designed for young users with the assistance of our teen and preteen volunteers is called "ThinkB4uClick," teaching them the consequences of their cyberactivities.

Marvel Entertainment, Inc. has also joined forces with WiredSafety.org to provide superhero assistance in educating our children and families on safer online practices. The first Internet safety comic, Internet Super Heroes meet the Internet Villains, teaches how Internet predators can infiltrate anyone's computer and wreck havoc on their lives by stealing their identity and posing as them online. Published under its exclusive license with Marvel, and sponsored by Microsoft, this first comic will help teach the 250,000 readers how to be smarter and safer online using Spider-Man, The Incredible Hulk and Dr. Doom, among others to bring the message to life.

WiredSafety.org also provides information and resources to help educate and guide law enforcement officers on Internet safety issues, crime prevention and investigation of cybercrimes. It has created a special website just for law enforcement officers, Cyberlawenforcement.org, also known as WiredCops.org. As part of the Wiredcops.org initiative, specially trained volunteers assist law enforcement in the investigation and prevention of trafficking of children, child pornography, child molestation, and cyberstalkers. Recently, at the request of leading law enforcement agencies, WiredSafety.org has begun using its teen volunteers to provide information that will assist undercover law enforcement officers in creating credible profiles of preteens and teens to help them become more effective when operating undercover online.

In addition to assisting law enforcement agencies, WiredSafety.org offers one-to-one assistance for victims of cyberabuse that may not arise to the level of a cybercrime and is not handled by law enforcement. WiredSafety's cyberhelpline gives "netizens" access to free help when they need it via the Internet. Its special team of helpline volunteers is assigned to cases and works one-to-one online to help resolve individual problems and get victims help when they need it. WiredSafety.org assists more cases of cyberharassment than any other organization in the world, helping thousands each month through its site and report line. Cyberbullying cases can be reported to the report line as well.

But when dealing with preteens and teens, the challenge has always been getting them engaged. Their "selective hearing" can get in the way of their learning safer and more responsible behavior online, just as it may at home. When approached, teens told us that we had to approach them with things that they consider important, using their language. So, WiredSafety.org recruited teens and preteens who help us do that. These expert Teenangels, 13 to 18 year olds, (and now their younger version, Tweenangels, from 9 - 12 years of age) deliver the message of safe, private, and responsible technology use to their peers. These youth-based programs were formed in 1999 to provide special perspectives and insight into how young people are using the new technologies and how to better prepare them to handle the risks they encounter.

Teenangels have been recognized and honored by Congress, Parliament, John Walsh, Time for Kids and recently, Teen People Magazine, among others. Their training is extensive and takes almost one year to complete. When they receive their "wings", however, they are true experts. It is the only Internet expert youth program in the world. And, once trained, these special teens and tweens help develop safer technologies, by providing expertise for and advising members of the Internet and entertainment industries, media and governmental agencies around the world.

Too often disconnected from the immediate consequences of their actions online, many “good” kids and teens find themselves doing things online they would never dream of doing in real life. This needs to change. The youth programs created by WiredSafety.org focus on cyberwellness and cyberethics which fits perfectly within its mission and expertise. To keep our children safe online, they need to understand the norms and rules of operating online. They must also recognize that they will be held accountable for what they do in cyberspace and that what they post online has ramifications beyond the momentary click. Teaching responsible technology use is crucial.

WiredSafety.org also offers a wide variety of educational and help services to the Internet community at large. Companies such as Disney, the Motion Picture Association of America, the National Sheriff's Association, Yahoo, Verizon Foundation, Marvel Comics, MySpace, Xanga, Johnson & Johnson, Google, Oracle, Facebook, Microsoft and AOL support and turn to Parry Aftab and WiredSafety.org for guidance and advice in dealing with Internet safety issues. Teenangels and Parry have testified before leading governmental and legislative bodies worldwide, including the U.S. Congress and the U.K. Parliament. Regulatory agencies, such as Singapore's Media Development Authority, the U.S. FTC and California's consumer protection arm have sought WiredSafety's and Parry's help. Their collaborative efforts with schools, community organizations, prosecutorial officers, local executive branch and law enforcement agencies, such as Alaska's Campfire USA, the Baltimore County public schools, Ohio's Wayne County Sheriff's office, the San Francisco DA, and Westchester County, NY's County Executive Spano, have affected hundreds of thousands of families worldwide. Using its unique expertise in the field, the charity also assists important trade associations, such as the CTIA (the wireless trade association) and the U.S. Sheriff's Association. WiredSafety.org also acts as a watchdog within most of the social networking websites, to help provide their users safety information and help when things go wrong.

Select volunteers find and review family-friendly Web sites, filtering software products, and Internet services. Some of the outreach team volunteers run programs, summits and also speak at local community groups and schools around the world teaching Internet safety, privacy and responsible use.

However, its work is not limited to the Internet alone. WiredSafety focuses on all aspects of interactive technology use and abuse. Its expertise includes cell phone safety and security, interactive gaming, social networking (mobile and online) and text-messaging products, as well as any new interactive technologies as they are developed. Its long years of working with Internet users and handling cybercrimes and abuse have created a flexible and knowledgeable volunteer force. If you can view content, communicate with others, spend money, or buy things using the technology, WiredSafety.org can help.

WiredSafety.org is headed by Parry Aftab, a mom, international cyberspace privacy and security lawyer and children's advocate. Parry is the author of the first book written for parents about Internet safety - The Parents Guide to the Internet (considered the bible of online safety and published in 1997) as well as The Parent's Guide to Protecting Your Children in Cyberspace (McGraw-Hill, 2000), which has been adapted and translated around the world. Her most recent books have been especially written and adapted for and published in England, China, Spain and Singapore. Her new book, Internet Safety 1-2-3, was released in December 2005 in Spain and will be released next year in the United States. And her new “Stop Cyberbullying!” guide launched in Spain in May 2006.

WiredSafety is proud of its reputation as the one-stop-shop for all cyberspace safety, privacy, security, and help needs. It is even prouder of the fact that all this can be accomplished without large government funding or money wasted on administration costs. No one is paid within WiredSafety.org. They are all unpaid volunteers - including

Parry herself. This all-volunteer workforce has been estimated at providing more than $3 million in unpaid services every year. Using a popular website and series of special topic sites, the organization has reached millions of Internet users since its inception and addresses more than 5000 children, teens and tweens and 1000 parents in person every month, on average.

WiredSafety.org mobilizes people of all ages who want to help others, and puts them to work doing just that. It is intent on its mission to "Take Back the Net!"

Appendix 2: Parry Aftab's Bio and CV:

Updated July 2006
Parry Aftab
Bio

Parry Aftab is a security, privacy and cyberspace lawyer, as well as an author, columnist and child advocate. A substantial portion of her time is donated to Internet issues involving children, from equitable access, to privacy, to safety, to helping develop quality and reliable content for children. She has also legally represented or acted as a consultant to most of the children's Internet industry, helping them comply with the law, while improving the Internet experience for children. When children and the Internet are concerned, Ms. Aftab's name is the first mentioned.

Parry Aftab is a worldwide leader in the area of online safety and parent and child Internet education. As Executive Director of WiredSafety.org, the oldest and largest online safety and educational program in cyberspace, Ms. Aftab helps prevent and assist law enforcement agencies in investigating cybercrime against children and families. Under its former name, her group was awarded the President's Service Award in October 1998 from the White House and Points of Light Foundation. Ms Aftab also works closely with law enforcement around the world to prevent cybercrimes and police the Internet and is part of the Home Office Cybercrime Task Force in the UK. She was recently appointed a Special Deputy Sheriff by Wayne County, Ohio's Sheriff, Thomas Maurer.

In 1999, Ms. Aftab was appointed by UNESCO to head up its child Internet sexual exploitation project for the U.S. She has also written the leading books for parents on Internet safety since her first book was published on the topic in December 1997.

Although her vocation was Internet security and privacy law, her avocation is children online – helping them become good cybercitizens and keeping them safe, private and secure online. She is dedicated to helping curb Internet-related crimes against children and assisting law enforcement in bringing the child predators to justice. Everyone who encounters Ms. Aftab is impressed with her passion and energy when children's Internet issues are involved.

While her passion is for protecting children from Internet sexual exploitation, she is also devoted to empowering them through access to the wonders of the Internet. She hopes to help all children become better informed and responsible cybercitizens, controlling the technologies instead of being controlled by them. Her programs are designed to teach them safe, private and responsible technology use, which includes teaching them good netiquette and respect for each other and the rights of others, including intellectual property rights of the music, movie, gaming and software industries.

Ms. Aftab was among the first in the world to devote her talents to keeping children safe online. She has helped design programs for parents and children in a wide range of Internet-related issues for ten years. Her work has been recognized by leading technology influencers, such as Family PC Magazine, when she was awarded Internet Pioneer of the Year in 2001. And child protection agencies have recognized her as well, when Child Abuse Prevention Services presented her with their 20th anniversary Community Leadership Award in 2005. (Past recipients of this award include Senator Clinton, Linda Fairstein, Judy Collins, Dr. Joyce Brothers and the "God Squad.")

Parry Aftab also provides parent Internet education and online safety content for such diverse sites as Nickelodeon, Children's Television Workshop, Disney, Microsoft, AOL, Yahoo!, Google, AT&T and MSNBC. She is a regular keynote speaker, and resource on camera for the media on diverse cybercrime, safety, privacy and cyberlaw

issues. She writes The Privacy Lawyer columnist for Information Week Magazine where she writes on a range of topics that affect technology, policy and privacy. Her expertise is especially in demand on children's Internet issues, because no one knows more about children online than Parry Aftab.

While she is devoted to protecting children online, Ms. Aftab seeks to empower children and their parents, not the censors. Her common sense approach to technology risks and solutions works as well anywhere in the world as it does in the United States. But what really makes her special is her ability to tap into the caring and creativity of young people to craft solutions that are written in their language and designed for their needs.

She is a frequent and respected resource for news programming and print journalists around the world. Her expertise has been featured nationally and internationally in online and print publications, including Readers Digest, Playboy, TV Guide Magazine, Cosmopolitan, People Magazine, Redbook, Biography, USA Today, Information Week, Working Women, Teen People, U.S. News & World Report, Family Circle, Newsweek, Ladies Home Journal, Smart Money Magazine, PC Magazine, Good Housekeeping, Better Homes & Gardens, Family PC Magazine, Yahoo! Internet Life, Information Week, CIO Magazine, The Wall Street Journal, The New York Times, The LA Times, most regional newspapers in the United States, The London Times Magazine, The Strait Times (Singapore), The South China Morning Post Sunday Magazine (Hong Kong), and more. As a result of her work online with children, Ms. Aftab was selected as a charter member of Children Television Workshop's Advisory Board, as well as appointed to The National Urban League's Technology Advisory Committee. In 2003 she was elected to TRUSTe's Board of Directors. She served on the advisory board for the Ad Council for two terms.

Parry Aftab has spoken to many governmental agencies and groups worldwide, conducted briefings for the U.S. Senate, testifies regularly before Congress, and has been a key speaker at the White House Summit on Online Content, the sole Internet-related expert speaking at the 2002 White House summit on Missing and Exploited Children and testified before leading legislative committees and The House of Lords, all with the same message: The Internet is a wonderful resource for families, and once parents understand the online risks, they can use common sense (and perhaps some filtering tools) to help their children enjoy cyberspace safely.

As one of the first lawyers in the world to specialize in Internet legal issues, Parry Aftab is admitted to practice law in New York and New Jersey. She attended law school at NYU School of Law where she received her J.D. degree. She received her B.A. degree as *Valedictorian* of Hunter College (having completed her full undergraduate degree in less than two years), where she was inducted into *Phi Beta Kappa*.

She resides in the New York metropolitan area and is a mother of two. Ms. Aftab can be reached at Parry@Aftab.com.

Parry Aftab

Professional Curriculum Vitae

Phone: 201-463-8663
parry@aftab.com

Internet privacy and security lawyer, licensed to practice law in NY and NJ,
The Privacy Lawyer columnist, author, consultant and public speaker
Executive Director of WiredSafety.org

AREAS OF EXPERTISE: Worldwide Cybercrime Protection and Prevention/Identity Theft/ Privacy, Data Collection and Security / Workplace Risk Management and Security/ Consumer Protection, Advertising and the Internet / E-Commerce/ Cyberstalking and Harassment/ Child Exploitation and Child Pornography, Children Online, Online Marketing, Cyber-workplace issues, Privacy training and coaching

---

CURRENT POSITIONS
President/CEO - Aftab Cyber-Consulting
Executive Director, WiredSafety.org (a 501c-3 corporation)
The Privacy Lawyer columnist for Information Week

EDUCATION

City University of New York Hunter College (Completed 4 yr degree in 2 yrs)	B.A., 1981 *Valedictorian* *Phi Beta Kappa* (Nu Chapter)
New York University School of Law	J.D., 1984

SELECT HONORS

Community Leadership Award, 2005
Awarded by Child Abuse Prevention Services

American Society of Business Publication Editors Award "Gold" O*riginal Web Commentary*
Informationweek.com for Parry Aftab's
"Patriotism, Compliance and Confidentiality" article

Activist of the Year Award, 2002
Awarded by Media Ecology Association

Internet Pioneer of the Year, 2001
Awarded by Family PC Magazine

Home Office, U.K.
Child Protection, Criminal Laws and Law Enforcement Task Forces

ORGANIZATIONS

TRUSTe
Member- Board of Directors (Elected December 2002)

Ad Council
Advisory Committee member (1999 - 2003)

Children's Television Workshop Online (Sesame Workshop)
Advisory Board (1998 – present)

UNESCO
President, U.S. National Action Committee, Innocence in Danger (appointed 1999)1998-present)

The Internet Society
Elected Chair, Internet Societal Task Force and Societal Steering Group (worldwide, 2001)
Member of Public Policy Committee ISOC (2001–present)
Chair, Privacy and Security Working Group of The Internet Society Task Force (2000-2001) appointed member since 1999

WiredSafety (wiredsafety.org) the world's largest Internet safety and help group, formerly functioned as "Cyberangels," recipient of President's Service Award, 1998,
Executive Director (1998-present)

The National Urban League
Technology Advisory Committee (1997 – present)

AUTHORSHIPS AND
RELATED ACTIVITIES

Author, selected books

Cyberbullying Guide (Spanish and English guide on preventing and dealing with cyberbullying)
Spain 2006

Internet con los menores Riesgos (Spanish guide for parents on Internet safety, especially written for Spain and South and Central America)
Spain 2005

Children and the Internet (official Chinese Internet safety guide)
China 2004

The Parent's Guide to Protecting Your Children in Cyberspace, McGraw-Hill,
(U.S. edition, January 2000; UK edition, March 2000; Singapore edition May 2000 and Spanish language US edition November 2000)

A Parents' Guide to the Internet, SC Press (October 1997)

Contributor, selected books

Child Abuse on the Internet.... Ending the Silence
(2001) Carlos A. Arnaldo, Editor
Chapter 21: The Technical Response: Blocking, Filtering And Rating The Internet - by Parry Aftab

The Best In E-Commerce Law
(2001) Warren E. Agin, Editor
Children's Online Privacy Law

Selected Speaking Engagements

WiredSafety's Social Networking Summit, June 2006

US Congress, Commerce Committee, Sub-Committee Investigations and Oversight, opening day hearings April 4, 2006

National Association of Independent School Annual Conference, March 2006

Stonybrook Cyberbullying Summit, September 2005

FDIC Conference on Security Online, August 2005

The Westchester County Cyberbullying Summit, February 8, 2005

The US Copyright Office – Luncheon Speaker (LA and SF events) February 2005

Child Abuse Prevention Service 20th Anniversary Luncheon Speaker, April 2005

FTC Workshop on P2P, December 2004

House of Commons – Parliamentary Briefing on Internet Safety, October 2004

IAPP (International Association of Privacy Professionals), June 11, 2004

EU- Safer Internet – Warsaw, March 2004

Media Development Authority- Singapore, Family Internet Week – March 15, 2004

Western Attorneys General Conference, July 29, 2003

Domain Day, Milan, Italy, November 5th, 2002

Wired Kids Summit, Washington D.C., October 15th, 2002 (Mediator and Host of the event at the Russell Senate Building)

White House Conference on Missing and Exploited Children, October 2nd, 2002 (Only panel speaker selected to discuss Internet issues). Other speakers included President George W. Bush, Colin Powell, John Ashcroft, Rod Paige and many distinguished others.

Council of Europe, Children's Online Safety, Belgium, November 2001

Microsoft, Privacy and Security Summit, Privacy Speaker, San Francisco, November 2001

Intellectual Property Organization, Featured Speaker on Internet Law, Privacy and Digital Rights, New York, November, 2001

SCOPE, Keynote Speaker, Cyber-terrorism, New York, October 2001

Rappateour, E.U. Online Content Regulation, Luxembourg, June 2001

Bertelsmann Foundation, Experts Meeting, Singapore, February 2001

Microsoft, Privacy and Security Summit, Speaker (only female speaker), Seattle, November 2000

Keynote Speaker, House of Lords, Kids Helping Kids, London (April 2000)

Keynote Speaker, Singapore Broadcasting Authority and Ministry of Information Conference, Children Online, Regulatory Issues, Singapore (November 1999, May 2000, February 2001)

Panelist, FTC Hearings on COPPA Regulations, Washington (June 1999)

Keynote Speaker, White House Summit, Online Content, Los Angeles (June 1998)

Keynote Speaker, C.A.R.U., Conference On Children's Online Privacy (September 1998)

Featured Speaker, Littleton Town Meeting hosted by Tom Brokaw and Jane Pauley, MSNBC (April 1999)

Appendix 3: Parenting Online (from WiredSafety.org)

Parenting Online

What do we do when our eight-year-old knows more than we do about cyberspace? How do we guide our children safely through this new world? How do we set the rules when we don't even understand the risks? The childproof locks, seatbelts and helmets we use to help keep them safe in everyday life won't protect them in cyberspace. There we need new and different gadgets and safety tips.

Welcome to the new world of parenting online! It's your newest challenge. But don't worry...it's not as hard as you think and it's well worth the effort.

Parenthood is never easy and the ground rules are always changing. We go from playing the role of confidante, to co-conspirator, to police chief, to teacher, to playmate and back...all in the same day. We barely have the chance to catch our breath!

The things we do to make sure our children stay safe are constantly changing too. When they crawl, we learn how to keep things off the floor. Then, they pull themselves upright, we have to keep them safe from the new dangers at eye level. Training wheels have to be removed, and we have to watch while they pedal away (generally into the nearest tree). We watch their sugar intake, make sure they take their vitamins and keep small items out of their mouths.

That's our job, as parents. So the tried and true warnings, passed down from generation to generation, are repeated... “don't talk to strangers...,” “come straight home from school...,” “don't provoke fights...,” “don't tell anyone personal information about yourself...” and “we need to meet your friends...” This is familiar territory after all. We know the dangers our kids face in the street or at the mall or in the school yard, because we faced them.

As in any large community, there are dangers our children encounter in cyberspace, too. But, since our children know more than we do about cyberspace, we worry about how we can teach them to avoid those dangers. Don't panic... those dangers can be managed using the same old warnings we've always used.

We just need to translate them into cyberspace terms...

And there are wonders around every cyber-corner too...

The Internet is the largest collection of information in the world, always available without a charge and delivered to your home computer. Every question you might have can be answered online. When your child asks you how deep the ocean is or why the sky is blue, you can “ask the Internet,” together.

You and your children can communicate with others too, worldwide and in every language, with the click of your mouse. Their artwork can be displayed, their news reporting published and their poems posted on the largest "refrigerator door" in the universe, where 700 million people can appreciate them.

You can research your family tree and build a family Web site. And, best of all...the most complicated homework assignment can be researched online (even last-minute on the Sunday night before it's due).

You can search online for just about anything and any information you want. The easiest way to do that is by using search engines. You can type your search into one of the search engines and often will find what you are seeking. Just as often, though, you will find sites that are trying to get your or your children's attention. Pornographers are the most frequent abusers of search engines, registering and coding their sites to trick people into visiting them, thinking they are Disney, Pokemon or even the White House.

Most of the search engines now have filtering options. By selecting one of these options, most inappropriate content is filtered out and the search results are typically kid-friendly. Two commercial search engines were designed just for kids, though, and are wonderful places to begin your child's search online. Yahooligans!, Yahoo! kid-sized search engine hand-selects the sites, making sure nothing slips through. It is best for younger children, ten and under. Ask Jeeves for Kids is Ask Jeeves kid-sized search engine. Although not as scrubbed clean as Yahooligans! hand-selected sites, it contains many more sites which make it perfect for slightly older children. I recommend it for children ten and older.

In addition, most full-size search engines have a filtered option you can select. But remember that even if you use a search engine filter, if the kids search for images, the can find things you wish they hadn't. That's when using a filtering product that can block images too might come in handy.

In addition to kid-sized search engines, there are many wonderful family-friendly site lists. WiredKids has one of its own, where the sites are selected and reviewed by our specially-trained volunteers. You can even recommend your favorite sites to be added.

There are some entertaining sites that teach children online safety, as well. Although we prefer our WiredKids.org, StopCyberbullying.org and InternetSuperHeroes.org the best, (she says modestly...) another very special one we want to point out. Disney's Surfswellisland.com teaches online safety Disney-style. Mickey Mouse, Donald Duck, Minnie Mouse and Goofy all find themselves involved in tropical island cyber-challenges relating to viruses, privacy, netiquette (cyber-etiquette) and responsible surfing. Lesson plans, online safety worksheets and other wonderful resources are all available without charge at the site.

Looking for homework help? Check out Discovery.com, Nationalgeographic.org, PBSkids.org and The National Gallery of Art kids page www.nga.gov/kids/kids.htm**.** And ask your school librarian or the librarian at your public library for sites they recommend. Librarians and library media specialists are the guides to valuable and safe online resources for children. And if you need something you can't find, send me an email at "Ask Parry," (askparry@wiredsafety.org) my Internet-syndicated online safety column. Drop by WiredKids.org or WiredSafety.org to find out how to submit a question.

CyberSense
...translating common sense for cyberspace

- **Don't talk to or accept anything from strangers.** That's the first one we learn while growing up, and the first one we teach our children. The problem in cyberspace though is teaching "stranger danger." Online, it's hard to spot the strangers.

  The people they chat with enter your home using your computer. Our kids feel safe with us seated nearby. Their "stranger" alerts aren't functioning in this setting. Unless they know them in real life, the person is a stranger no matter how long they have chatted online. Period. You need to remind them that these people are strangers, and that all of the standard stranger rules apply.

  You also must teach them that anyone can masquerade as anyone else online. The "12-year-old" girl they have been talking to may prove to be forty-five year old man. It's easy for our children to spot an adult in a schoolyard, but not as easy to do the same in cyberspace.
- **Come straight home after school.** Parents over the generations have always known that children can get into trouble when they wander around after school. Wandering aimlessly online isn't any different. Parents need to know their children are safe, and doing something productive, like homework. Allowing your children to spend unlimited time online, surfing aimlessly, is asking for trouble.

  Make sure there's a reason they're online. If they are just surfing randomly, set a time limit. You want them to come home after they're done, to human interaction and family activities (and homework).
- **Don't provoke fights.** Trying to provoke someone in cyberspace is called "flaming." It often violates the "terms of service" of your online service provider and will certainly get a reaction from other people online.

  Flaming matches can be heated, long and extended battles, moving from a chat room or discussion group to e-mail quickly. If your child feels that someone is flaming them, they should tell you and the sysop (system operator, pronounced sis-op) or moderator in charge right away and get offline or surf another area. They shouldn't try to defend themselves or get involved in retaliation. It's a battle they can never win.
- **Don't take candy from strangers.** While we don't take candy form people online, we do often accept attachments. And just like the offline candy that might be laced with drugs or poisons, a seemingly innocent attachment can destroy your computer files, pose as you and destroy your friends or spy on you without you even knowing it. Use a good anti-virus, update it often and try one of the new spyware blockers. You can get a list of the ones we recommend at WiredSafety.org. Practice safe computing!

- **Don't tell people personal things about yourself.** You never really know who you're talking to online. And even if you think you know who you are talking to, there could be strangers lurking and reading your posts without letting you know that they are there. Don't let your children put personal information on profiles. It's like writing your personal diary on a billboard.

  With children especially, sharing personal information puts them at risk. Make sure your children understand what you consider personal information, and agree to keep it confidential online and everywhere else. Also teach them not to give away information at Web sites, in order to register or enter a contest, unless they ask your permission first. And, before you give your permission, make sure you have read the web site's privacy policy, and that they have agreed to treat your personal information, and your child's, responsibly.
- **We need to get to know your friends.** Get to know their online friends, just as you would get to know their friends in everyday life. Talk to your children about where they go online, and who they talk to.
- **R-E-S-P-E-C-T.** We all know the golden rule. We have a special one for cyberspace. Don't do anything online you wouldn't do offline. If you teach your child to respect others online and to follow the rules of netiquette they are less likely to be cyberbullied, become involved in online harassment or be hacked online. You can learn more about the ways to combat cyberbullying at our new website, StopCyberbullying.org or at WiredSafety.org's cyberstalking and harassment section. Remember that it is just as likely that your child is a cyberbully (sometimes by accident) as a victim of one. Let them know they can trust you not to make matters worse. You have to be the one they come to when bad things happen. Be worthy of that trust.

Remember that the new handheld and interactive gaming devices you buy have real risks to. Your children can send and receive text-messages from anyone on their cell phones or text-messaging devices and interactive games allow them to chat, on Internet phone, to anyone who wants to talk with them. The new Bluetooth devices let your child receive messages form anyone in a 300 foot range, and could be a problem if they play the new Bluetooth handheld games in a mall. Think about the features you are buying when you buy new devices for your children. Check into privacy and security settings. Our Teenangels (teenangels.org) are working on new guides for parents and other teens on what to look for and think about before you buy a new interactive device. Look for them at your local retailer or on the WiredSafety.org and Teenangels.org websites.

Don't just set up the computer in the corner of their bedroom, and leave them to surf alone. Take a look at their computer monitor every once in awhile, it keeps them honest. Sit at their side while they compute when you can. It will help you set rules that make sense for your child. It also gives you an unexpected benefit...you'll get a personal computing lesson from the most affordable computer expert you know!

And it's worth the effort. When our children surf the Internet, they are learning skills that they will need for their future. They become explorers in cyberspace, where they explore ideas and discover new information.

Also, because there is no race, gender or disability online, the Internet is the one place where our children can be judged by the quality of their ideas, rather than their physical attributes.

What Tech Tools Are Out There?

Blocking, filtering and monitoring...when you need a little help

There are many tools available to help parents control and monitor where their children surf online. Some even help regulate how much time a child spends playing computer games, or prevent their accessing the Internet during certain preset times.

I've listed the type of protections that are available. But, most of the popular brands now offer all of these features, so you don't have to choose. Recently, given parents' concerns about strangers communicating with their children online, monitoring software has gained in popularity. Although it might have its place in protecting a troubled child, it feels more like "spyware" than child protection. But it's ultimately your choice as a parent. The newest trend is to use products supplied by your ISP called parental controls. AOL's parental controls were the first of these to be developed and used. MSN 8.0 launched the first set of parental controls for MSN. To read more about the various products and services we have reviewed, visit WiredKids.org and WiredSafety.org.

Blocking Software

Blocking software is software that uses a "bad site" list. It blocks access to sites on that list. They may also have a "good site" list, which prevents your child from accessing any site not on that list. Some of the software companies allow you to customize the lists, by adding or removing sites from the lists. I recommend you only consider software that allows you to customize the list, and lets you know which sites are on the lists.

Filtering

Filtering software uses certain keywords to block sites or sections of sites on-the-fly. Since there is no way any product can keep up with all the sites online, this can help block all the sites which haven't yet been reviewed. The software blocks sites containing these keywords, alone or in context with other keywords.

Some companies allow you to select certain types of sites to block, such as those relating to sex, drugs or hate. This feature engages special lists of keywords that match that category. As with the "bad site" lists, the lists of keywords used by the filtering software should be customizable by the parent, and every parent should be able to see which terms are filtered.

Outgoing Filtering

No... this doesn't mean your software had a sparkling personality :-) (that's cyberspace talk for "grin" and means you're supposed to smile at my brilliant humor, and if you want to learn more about this stuff...you need to read my Ms. Parry's Guide to Correct Online Behavior). It means that your child won't be able to share certain personal information with others online. Information such as your child's name, address or telephone number can be programmed into the software, and every time they try to send it to someone online, it merely shows up as "XXXs." Even with kids who know and follow your rules, this is a terrific feature, since sometimes, even the most well-intentioned kids forget the rules.

Monitoring and Tracking

Some software allows parents to track where their children go online, how much time they spend online, how much time they spend on the computer (such as when they are playing games) and even allows parents to control what times of day their children can use the computer. This is particularly helpful when both parents are working outside of the home, or with working single-parents, who want to make sure their children aren't spending all of their time on the computer. Many parents who don't like the thought of filtering or blocking, especially with older children and teens, find monitoring and tracking satisfy their safety concerns. They can know, for sure, whether their children are following their rules.

We particularly recommend using a monitoring software and then forgetting it's installed. Think of it as the security video camera in the corner of the bank. No one views the tapes until the bank is robbed. If something bad happens, you can play back the monitoring log and see exactly what occurred, and who said what, and in dire situations,

where your child went to meet an adult offline. We particularly like Spectorsoft.com, because their products can monitor all instant messaging platforms, which is key to keeping your children safe online.

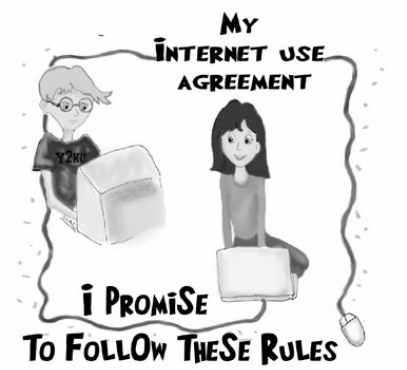
Parents have to remember, though, that these tools are not cyber-babysitters. They are just another safety tool, like a seat belt or child safety caps. They are not a substitute for good parenting. You have to teach your children to be aware and careful in cyberspace. Even if you use every technology protection available, unless your children know what to expect and how to react when they run into something undesirable online, they are at risk. Arming them well means teaching them well.

Your Online Safety "Cheatsheet"
Some Basic Rules for You to Remember as a Parent . . .

- Make sure your child doesn't spend all of her time on the computer. People, not computers, should be their best friends and companions.
- Keep the computer in a family room, kitchen or living room, not in your child's bedroom. Remember that this tip isn't very helpful when your children have handheld and mobile Internet and text-messaging devices. You can't make them keep their cell phones in a central location. So make sure that the "filter between their ears" is working at all times.
- Learn enough about computers so you can enjoy them together with your kids.
- Teach them never to meet an online friend offline unless you are with them.
- Watch your children when they're online and see where they go.
- Make sure that your children feel comfortable coming to you with questions and don't over react if things go wrong.
- Keep kids out of chat rooms or IRC unless they are monitored.
- Encourage discussions between you and your child about what they enjoy online.
- Discuss these rules, get your children to agree to adhere to them, and post them near the computer as a reminder.
- Find out what e-mail and instant messaging accounts they have and (while agreeing not to spy on them) ask them for their passwords for those accounts.
- "Google" your children (and yourself) often and set alerts for your child's contact information. The alerts will e-mail you when any of the searched terms are spotted online. It's an early warning system for cyberbullying posts, and can help you spot ways in which your child's personal information may be exposed to strangers online. To learn how to "Google" them, visit InternetSuperHeroes.org.
- Teach them what information they can share with others online and what they can't (like telephone numbers, address, their full name, cell numbers and school).
- Check your children's profiles, blogs and any social-networking posts. Social-networking websites include myspace.com, facebook.com and xanga.com. (We work closely with MySpace and Facebook to help keep their users safer.) Social networks, generally, shouldn't be used by preteens and should be only carefully used by teens. Yfly.com is a new teen-only social network that is designed from top to bottom to keep teens safer and teach them about more responsible behaviors.
- For those of you with preteens and young teens, read the Safer Social Networking guide at WiredSafety.org.
- Get to know their "online friends" just as you get to know all of their other friends.
- Warn them that people may not be what they seem to be and that people they chat with are not their friends, they are just people they chat with.
- If they insist on meeting their online friend in real life, consider going with them. When they think they have found their soul mate, it is unlikely that your telling them "no" will make a difference. Offering to go with them keeps them safe.
- Look into the new safer cell phones and cell phone features that give you greater control over what your children can access from their phone and how can contact them.

PARENTING ONLINE

MY AGREEMENT ABOUT USING THE INTERNET



Once you understand enough about cyberspace and how your children surf the Internet, you can set your own rules. These are the basic rules, even though you may want to add some of your own.

Some kids like setting the rules out clearly in an agreement. Here's one you can use, and post near your computer to help them remember how to surf safely. (Note that while the tips may work for teens, the contract is designed for preteens and younger.)

I want to use our computer and the Internet. I know that there are certain rules about what I should do online. I agree to follow these rules and my parents agree to help me follow these rules:

1. I will not give my name, address, telephone number, school, or my parents' names, address, or telephone number, to anyone I meet online.
2. I understand that some people online pretend to be someone else. Sometimes they pretend to be kids, when they're really grown ups. I will tell my parents about people I meet online. I will also tell my parents before I answer any e-mails I get from or send e-mails to new people I meet online.
3. I will not buy or order anything online without asking my parents or give out any credit card information.
4. I will not fill out any form online that asks me for any information about myself or my family without asking my parents first.
5. I will not get into arguments or fights online. If someone tries to start an argument or fight with me, I won't answer him or her and will tell my parents.
6. If I see something I do not like or that I know my parents don't want me to see, I will click on the “back” button or log off.
7. If I see people doing things or saying things to other kids online I know they're not supposed to do or say, I'll tell my parents.
8. I won't keep online secrets from my parents.
9. If someone sends me any pictures or any e-mails using bad language, I will tell my parents.
10. If someone asks me to do something I am not supposed to do, I will tell my parents.
11. I will not call anyone I met online, in person, unless my parents say it's okay.
12. I will never meet in person anyone I met online, unless my parents say it's okay.
13. I will never send anything to anyone I met online, unless my parents say it's okay.
14. If anyone I met online sends me anything, I will tell my parents.
15. I will not use something I found online and pretend it's mine.
16. I won't say bad things about people online, and I will practice good netiquette.
17. I won't use bad language online.
18. I know that my parents want to make sure I'm safe online, and I will listen to them when they ask me not to do something.
19. I will help teach my parents more about computers and the Internet.

20. I will practice safe computing, and check for viruses whenever I borrow a disk from someone or download something from the Internet.
21. I won't post my cell number on my away message, and will check with someone before posting something personal about me on my blog or on a networking site.
22. I will Stop, Block and Tell! If I am harassed online or cyberbullied.
23. I will Take 5! before reacting to something that upsets me or makes me angry online.
24. I will practice responsible "thinkB4Uclick" rules. (I know I can find out more about these things at InterentSuperHeroes.org and StopCyberbullying.org.)
25. I will learn how to be a good cybercitizen and control the technology, instead of being controlled by it.

_____

I promise to follow these rules. (signed by the child)

_____

I promise to help my child follow these rules and not to over react if my child tells me about bad things in cyberspace (signed by parent).

From Parry:

I am asked questions about kids online safety at least a hundred times a day. Is the Internet a dangerous place? Are there predators out there looking to set up a meeting with my child? How can we find good and reliable content online? How can I supervise my child's surfing when I can't even turn on the computer?

These any other question like these fill my inbox daily. (If you have a question of your own, visit WiredKids.org or WiredSafety.org and click on "Ask Parry." Here is the one simple answer:

The single greatest risk our children face in connection with the Internet is being denied access. We have solutions for every other risk.

That bears repeating, over and over, especially when we hear about Internet sexual predators, hate, sex and violence online. But our children need the Internet for their education, careers and their future.

Happily, most of the risks are easily confined. In each and every case when children encounter Internet sexual predators offline, they go willing to the meeting. They may think the person is a cute fourteen year old girl or boy, but they know they are meeting someone they don't know in real life. That means we can prevent 100% of these crimes. Merely teach our children not to meet Internet strangers offline. If they are set on meeting that person anyway, go with them. That way, if the person turns out to be a cute fourteen year old, you are the hero. And if they aren't, you're an even *bigger* hero.

Our WiredKids, WiredTeens and Teenangels programs, in addition to being fun and educational sites, are also volunteer programs where children and teens are taught online safety and privacy and responsible surfing. They then use these skills to help other children and teens learn to surf safely, as well. Talk to your children about what they do online (and offline also), and let them know you are there to help if things go wrong. You will note that in our safe surfing agreement parents have to promise only one thing...not to overreact if their children come to them for help. Earn their trust, and be worthy of it. Register your children at WiredKids.org, our children's online safety site, and we will make sure they learn what they need to know about enjoying the Internet safely and privately. It's not about technology at all...it's about communication and good parenting.

Remember, we're all in this together!

Parry
Parry Aftab, Esq.
Executive Director
WiredSafety.org and its family of sites and programs, including Teenangels.org, WiredKids.org and CyberLawEnforcement.org

WiredSafety is a 501c-3 non-profit organization formed under the laws of the State of New York. (Its legal name is "Wired Kids, Inc.") This publication is copyrighted to Parry Aftab, Esq. All rights reserved. For permission to duplicate this publication, contact parry@aftab.com.

Appendix 3 and Appendix 4
WiredSafety.org's Print PSAs

Even small bits of personal information that you share online can come back to haunt you. It doesn't take much. Kids are especially vulnerable. They're innocent, trusting and want to make new friends - and sometimes they can be a little careless. A phone number, a photo, last name, the name of their school or team - even completing an online contest entry form at the wrong site - can result in identity theft, stalking or worse. So make sure you tell them what not to say online.

The more information you give your kids, the less information they'll give a stranger.

wired SAFETY

WiredSafety.org

The world's largest Internet safety, help and education organization

MR. WHITFIELD. Thank you. Thank you so much, Ms. Aftab. And Ms. Sullivan?

MS. SULLIVAN. Thank you, Mr. Chairman. Good afternoon. My name is Shannon Sullivan. I am 14 years old and I will be entering tenth grade in the fall. Teenangels is a group of 13 to 18-year-old volunteers that have been specially trained by the local law enforcement and many other safety experts in all aspects of online safety, privacy and security. We go through extensive training by Parry Aftab, Executive Director of WiredSafety.org. Teenangels was founded in 1999 in New Jersey, and I

have been a part of the program since I was 13. We are more than just teens who learn how to use the Internet and other interactive technologies safely. We are experts who advise many leading corporations. It is a great program because it is not teachers or parents just telling you another thing you shouldn't be doing. It is your friends, another teen, someone who is in the same situation you are and understands the trends and what all teens want to do.

An interesting fact about Teenangels is that there are more Teenangels in the State of New Jersey than any other State in the country or any other place in the world. More of us means more teens being taught about Internet safety, more parents aware of the dangers of the Internet, and a lot more teachers and schools involved in our fight for a safer Internet for people of all ages. The fact is, kids do stupid stuff on the Internet. They pose in appropriate pictures, post personal information, and speak to people they do not really know. But the answer is not getting rid of social networking. Social networking is here to stay. I am sure it has become a part of your teens, or teens you know, lives and an essential communication for people of all ages.

WiredSafety is working with websites, law enforcement, parents, and schools to help create a total solution. We do not want to get rid of social networking, but there are so many ways to make it safer and more kid and teen-orientated to protect our children. There is not one answer to solving the problems of social networking. Everyone needs to work together in order to solve the problem and to make sure social networking has more benefits than dangers. One answer is teaching. It is our job as Teenangels, and your job as elected officials, teachers, and parents, to inform all kids of what not to do and what they are allowed to do on the Internet. We explain the dangers and the consequences of posting personal information, posing in inappropriate pictures, and speaking to people they do not know in real life, the teens, then they will be a lot of safer on the Internet.

The problem is, not enough teens understand the dangers. They do not believe it will ever happen to them. But the fact is, it can happen to anyone. And a lot of parents are unaware and are almost afraid of finding out what their kids are doing. They feel very uncomfortable when using a computer. Parents need to know what their kids are doing on the Internet. Now, when a parent tells a teenager, or my mom tells me something to do, I am not necessarily going to listen or take it as seriously as when my peer or another teen tells me what to do.

Learning from your mistakes. When I was in eighth grade my friend set me up with a profile on myspace.com. All my friends have profiles and I figured it would be a good way to connect with my friends. So on my page I had my picture, my first and last name, my age and school I

attended and what year I was graduating. I had no idea that it wasn't just my friends looking at my pages; anyone who wanted to. Any predator who was looking for a 13-year-old girl from Woodbridge, New Jersey, could easily find one. I learned from my mistake and I understand that anything posted on the Internet can be seen by anyone at any time. But teens need to learn from my mistake. As we get teens to come out and tell their stories, either about how they have gotten in trouble on the Internet or about the mistakes they have made, then other teens would learn from what they did and not make the same mistake.

So what do we need to do? As well-informed teens, elected officials, teachers, and parents, it is our job to teach kids and teens about the dangers of the Internet, inform parents about what their children are doing on the computer, and give teachers and schools options about how to deal with social networking and each coming trend on the computer. The Internet is a great learning tool and it is great for people of all ages to use. But if not used properly, it can become extremely dangerous and hazardous to our children's lives. So if we all come together and work to make the Internet safer and teach today's teens and tweens how to be safer, then the Internet will stay as a great learning tool and a vital part of our lives. Thank you.

[The prepared statement of Shannon Sullivan follows:]

PREPARED STATEMENT OF SHANNON SULLIVAN, TEEN ANGEL, WIREDSAFETY

Opening Statement:

Thank you for inviting me here today to share information about Teenangels, WiredSafety.org and how we can protect everyone online. My name is Shannon Sullivan, and I am 14 years old from New Jersey. I will begin 10th grade in the fall. I have been a Teenangel for one year. I became one after my mother found out I had a MySpace. I had the opportunity of testifying before this sub-committee on the opening day of the hearings in Washington, following the testimony of Justin Berry.

I have recently been honored by Teen People Magazine as a representative of Teenangels for our role in helping change the world. That is a big challenge. But it is one that teens can live up to.

Teenangels are more than teens who learn how to use the Internet and other interactive technologies more safely. They are experts who advise many leading corporations. They have become well-known for their special insight into technology from a teen's perspective. Teenangels now advise major corporations on Internet and technology uses, including Disney, the CTIA, Microsoft, AOL, Yahoo!, Marvel and others. They assist law enforcement agencies in designing more effective undercover investigation methods. They work with large industry groups, such as the Motion Picture Association of America, in building educational programs and public service messages.

They have helped create safer interactive gaming technologies, safer cell phone features and more secure social networking programs. They have hosted briefings at the House of Parliament, conducted training for law enforcement agencies and written articles for leading magazines. They do presentations within their community for parents, students and senior citizens on safe use of the Internet and new interactive technologies.

They spend a great deal of time on Internet sexual predators issues, anti-piracy and cyberbullying. We teach good cybercitizenship and responsible technology use, not only safety and privacy.

Teenangels are 13-18 year olds who train in all aspects of Internet and interactive technology safety, security and responsible use. (Tweenangels is the younger and lighter version of Teenangels, comprised of 9 to 12 year olds.) Once we are trained by Parry Aftab, leading law enforcement agencies and industry leaders around the world, these special teen experts create their own programs to teach safe and responsible technology use.

Some Teenangels are technological experts, creating animations, Flash applications, videos and computer games that help deliver their messages. Others concentrate on law and policy. Many have good public speaking, research or writing skills. The best thing about Teenangels is that it helps young people develop their own talents and help others at the same time.

We challenge teens and preteens, "Think you know more than most adults about the Internet? Share what you know, and learn more from the experts. Be part of the solution. Be a Teenangel!"

It is important that we teach young people that being safe isn't lame. That it's not cool to pretend you were out drinking all weekend, or to pose in your bra online. Many teens and preteens are lying about their ages to use social networking websites. And when they are there, they are often doing high risk things. But, it's important that parents understand that most teens and preteens are using the technology safely and responsibly. We just need to address them in our own language.

Recently, Teenangels began working with Nick Lachey. When Parry wasn't able to attend a luncheon with Teen People introducing me (she was in Spain launching her new book), Nick came instead. He learned that Internet sexual predators were using his name to lure teens into sending sexual pics online. Since he first met Parry he has donated his time to helping us keep kids safer. He is even helping us with public service announcements and a fun new animated educational series we are producing using Teenangels to teach safer and more responsible technology use.

Teenangels is now working with Nick's new site, YFly.com, to help create a safer teen social networking site. We helped create Don't Be Stupid to teach teens that engaging in reckless behavior online is stupid, not cool.

As Teenangels, we have the mission of helping make the Internet safer. We need your help to do that. First I would like to thank you for helping us by providing funding. We just received an earmark from Congress, through the Department of Justice, for $50,000. Since Teenangels hold bake sales and wash cars to raise money for our programs, this will change our world. We cannot thank you enough!

Next, I would like to share thoughts about what we can all do to help keep young people safer online.....

Why Teenangels works and how teens can help keep each other and themelves safer online:

- We are more than just teens who learn how to use the Internet and other interactive technologies safely. We are experts who advise many leading corporations
- It is a great program because its not teachers or parents just telling you another thing you shouldn’t be doing, instead it’s your friend, another teen, someone who is in the same situation you are and understands the trends and what all teens want to do.
- And an important part about TeenAngels is that there are more TeenAngels in state of New Jersey than any other state in country, or any other place in world

- More of us means more teens being taught about internet safety, more parents aware of the dangers of the internet, and a lot more teachers and schools involved in our fight for a safer internet for people of all ages

Kids do stupid things on the internet, we need to recognize that if we are going to try and address the problem:

- Pose in inappropriate pictures
- Post personal information
- Speak to people they don't really know

The answer is not getting rid of Social Networking

- Social Networking is here to stay
- I'm sure it has become a part of your teen's or teens you know lives
- It is the central communication for people of all ages
    - Bands posting when shows are

How Wiredsafety can help...

- WiredSafety is working with websites, law enforcements, parents, and schools to help create a total solution
- We don't want to get rid of social networking but there are so many ways to make it safer and more kid and teen orientated to protect our children
- There is not one answer to solving the problems with social networking
- Everyone needs to work together in order to solve the problems and to make sure social networking has more benefits than dangers
- And our Executive Director lives here in NJ too!

One answer is teaching kids and teens to thinkb4uclick!

- It is our job as TeenAngels and your job as elected officials, teachers, and parents to inform all kids of what not to do and what they are allowed to do on the internet
- If we explain the dangers and the consequences of posting personal information, posing in inappropriate picture, and speaking to people they do not know in real life to teens they would change their behavior and be a lot safer on the internet
- The problem not enough teens understand the dangers, they don't believe it will ever happen to them, but the fact is it can happen to anyone
- And a lot of parents are unaware and are almost afraid of finding out what their kids are doing. They feel very uncomfortable when using the computer. Parents to know what their kids are doing on the internet.
- Now when a parent tells a teenager or my mom tells me something to do I'm not necessarily going to listen or care as much as when my peer or another teen tells me to do something.

Learning from your mistakes

- When I was in 8th grade my friend set me up with a profile on myspace.com (tell story)
- I learned from my mistake and I understand that anything posted on the internet can be seen by anyone at anytime but teens need to learn from my mistake
- If we got teens to come out and tell their stories either about how they got in trouble on the internet or about the mistakes they've made then other teens would learn from what they did.

So what we need to do

- As well informed teens, elected officials, teachers, and parents its our job to teach kids and teens about the dangers of the internet, inform parents about what their children are doing on the computer, and give teachers and schools options about how to deal with social networking and each coming trend on the computer

Closing

- The internet is great learning tool and is great for people of all ages to use but if not used properly it can become extremely dangerous and hazardous to your children's lives. So if we all come together and work to make the internet safer and teach today's teens and tweens how to be safer than the internet will stay as a great learning tool for people of all ages.

Thank you for your time and caring enough to hold this hearing. And thank you for taking the time to listen to teens. It's nice to be included. And I will remember this day forever. On behalf of all my fellow Teenangels and Tweenangels, thank you.

Shannon Sullivan, age 14
New Jersey
Teenangels.org

Appendixes

Appendix A: (from Teenangels.org)

Safety Tips From the Mouths of Teenangels

(The Real Experts)...

While we have more extensive safety tip lists in Parry's book, here is a summarized version of the tips we thought were most important!

As Teenangels, safety is our biggest concern. So here are some tips and ideas that we and others have to share. Some of the best suggestions come from TEENS, just like you!

If you have a safety tip or story of something that has happened to you and how you handled it, please send it to us. We would love to hear from you! Email Teenangels.

Thoughts for Parents, Teens & Kids from the Teenangels

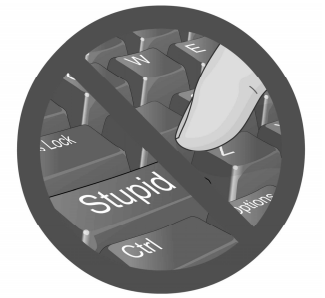
Parents... Don't be afraid of the Internet. It's an extremely useful tool & can't be dismissed because it is new & sometimes confusing. The Internet can be an excellent way for you & your children to bond & share a common interest. Be open with your kids & get involved. Most of all, learn all that you can about being safe, keeping your child safe, & taking advantage of the Internet's myriad uses. Tell your children not to be afraid to come to you with problems of any kind.

Teenagers...Although the Internet is a great way to meet new people, do research, and chat with friends, there are dangers. Be aware of these dangers. Always use common sense. Although you may think that bad things won't happen to you, they most certainly can. Be open with your parents about what you do online. Don't meet people offline that you met online! Make sure a site is secure and trustworthy before giving in your personal information. Obey the law and don't steal music, motion pictures and software! Balance the time you spend online and offline. Remember your friends in real life and don't take them for granted. Go outside & enjoy life beyond cyberspace.

Kids... While it's great to chat with people in kid-safe chat rooms online, you should spend time with friends in real life. School, family, & friends should always come before the Internet. Always tell your parents about what you do online. Let them sit with you, & teach them about the Internet. When they do sit with you, don't get mad at them. Just know they care about you & don't want to see you hurt in any way. Always remember that people online don't always tell the truth. Don't give out a lot of information about yourself. If anything bad ever happens to you on the Internet, always tell your parents or someone you trust. Always remember that it's never your fault.

Appendix B: Don't Be Stupid!

For Teens:



Don't Be Stupid!

What you need to know about cyberdating and staying safe

The Downers:

You never really know who someone is online. They may sound hot and their pic may be even hotter, but they could be someone you don't expect. They could be your little brother's snotty 12-year old friends having fun at your expense. Or three 15-year old mean girls posing as a heart throb to set you up for humiliation. Or they could be some 47 year old pervert. Either way, who needs it?

And even if it is a cute 16-year old guy or girl, there is no guarantee that when things are over, that sexy pic you shared with them won't end up on some website or profile somewhere. Or they could use the password you shared with them to change your profile, pose as you and harass your friends or even lock you out of your own account. Or they could cyberbully, flame, cyber-harass or cyberstalk you or your friends…When you breakup, all bets are off!

The Buck Stops Here...You Need to Protect *Yourself* Online

Smart teens have been fooled by slimy adults posing as teens. There is no safe way to meet someone you only know online, (with maybe from a few phone calls to help), in RL. If you're thinking about meeting someone, think again. Talk to your friends. Check out Katiesplace.org and learn about how others have been hurt by adults posing as teens. Smart teens like you. Don't do it!

We can't emphasize this enough! But, we also know that if you are convinced that this is a cute 16 year old boy or girl is the love of your life and destined for you from birth, you may ignore this advice and plan on meeting them in RL. If you are intent on taking this risk, do what you can to minimize it. Make sure you follow these Don't Be Stupid tips:

1. Don't disclose too much personal info. Start by assuming that the person on the other end is a predator. That means no full names, street addresses, RL schedules or telephone numbers that can be reverse searched (check it out online or where you work, or similar info about your friends that can be used to find you offline. It's always a good idea to use a disposable e-mail address or IM account, something you set up just for this and that you can drop if things start going downhill (like yahoo, hotmail or MSN.) Make sure that this new screen name doesn't give away any information about who you are in RL either (Tiff1991@[fill in the blank]).

2. Play detective. Photos can give away more information than you ever intended. Things in the background of the photo, like the license plate on your car, your house, the store where you work, the school or camp sweatshirt you're wearing or a pic with you in front of your school can be risky. So can photos posted by your friends. While you may be very careful about what you are sharing online, they may not be as careful. If you link to their profile and haven't told anyone where you live, but they post their best friends (including you), everyone can now figure out what town you live in and where you go to school. They just need to cross-reference a bit. The same thing happens with everything you or your friends post. Look over your profile and the profile of your friends. If you were a detective for Law & Order, could you find yourself in RL? If so, change whatever

is giving too many clues away. Password protect it and guard your password, and ask your friends to do the same. Start a rule - never post info about a friend or their pic without asking first.

3. Say Cheese! There are three issues about pics online - posting something you'll regret, shooting a lame pic or posting a pic that can be abused or misused by others. Sometimes to get attention, teens pose in provocative ways or snap a pic when they are doing things their parents would not want to see. Unfortunately, parents do see them. And so do principals and predators (and shortly college admission staff).

We all know that lame "MySpace" pose - bad lighting, cheeks sucked in, lips pursed, head tilted up, with a flash in the mirror. :-) Is that really how you want to be remembered?

Putting your best foot forward and using a good pic or a fun one is much better than doing the "I am so hot I can't stand it" pose. Boys posing shirtless and trying to make their pecs look bigger by crossing their arms underneath them, or girls posing in a bikini top (or worse) or very low cut pants will get you attention. But not the attention you may want. And cyberharassment where an innocent G-rated pic is manipulated and used to make you look bad or to morph your head on someone else's naked body is commonplace. You can avoid that by using photo-editing software to pixilate or blur the image, turn it into a sketch or cartoon, sepia or black and white. This makes your photos harder to abuse and less attractive to the harasser or a predator.

Our new Best Food Forward (BFF) tips teach you how to make the impression you want to make, without being lame or stupid. You can read about them at Teenangels.org or at our Don't Be Stupid tips at YFly.com. These will help you come across the way you want to online.

4. **Look for the red flags.** Beware of others online who:

- ask too many questions
- post things that don't make sense
- move too fast
- promise you ridiculous things (if it seems too good to be true, it's not true!)
- like everything that you like, exactly the way you like it
- know too much about you
- engage in cybersex
- just don't feel right or make you uncomfortable
- are evasive
- can't keep their story straight
- initiate sexual conversation or innuendo
- don't know the things most teens know (just know the experienced predators make it their business to know these things)
- pressure you to send sexy pics or meet in RL
- give you the creeps

5. ThinkB4UClick. It's so easy to do things online that you would never do in RL. You don't have to look the other person in the eye. No one else is there to tell you to cool it. You are stronger, smarter, more empowered and braver online. You may not like your coach, principal or former best friend or boy or girl friend.

You take their pic and morph it onto someone else's naked body. You post sex ads using their name and contact info. Maybe you take a pic of them with your cell phone in a locker room, bathroom, at a slumber party or in the changing room at the Gap. You build a profile telling everyone what a slut they are, or post these pics online anonymously. Or you send sexual images of yourself to someone you like, thinking they will want to go out with you if they see how sexy you are. They don't, but share the pic

with their fifty nearest and dearest friends - who show it to their friends and so on and so forth....

You think no one can find you, trace you or figure out who you are (you're wrong!). There is nothing between your impulse and your click...no time to think about it, no time to calm down. No time to use the "filter between your ears."

You are also typing fast and aren't proofreading your text-messages, IM or posts, and often send it to the wrong person on your buddy list or misspell their screen name. You may forget to type in "jk" or the word "not." You may find yourself in trouble without knowing why. Think R-E-S-P-E-C-T! (Now do it like Aretha, with lots of style!) Taking that extra second to make sure you send it to the right person, aren't misunderstood and are willing to be accountable for what you are doing and saying online is crucial. It will save you lots of grief later!

Appendix C

For Teens:

Finding Love in all the Cyberplaces...Don't Be Stupid!

If you decide to meet someone in-person, and ignore everything we taught you -- at least follow these tips and trust your gut. If something feels wrong, get out of there and report it. And remember that about 30% of the victims are boys. They just don't report it. So be careful!

1. Go public. Find out what they will be wearing and arrange for a place to meet. Then get there early and stake things out. The idea is to spot them before they spot you. Make sure that you meet in a well-lighted public place. It should be big and public enough so you can he help if you needed it, but not so big, crowded and noisy that you wouldn't be heard or couldn't get help. Don't meet in an amusement park, where screaming is part of the scenery. A mall is a good choice, but sit back and watch and see who shows up. If they are not what was promised, run...do not walk...home, to the security office or to the local police department. Make sure someone calls the police.

Never meet at your place or theirs. Never get in a car with them. Go with lots of friends (preferably Sumo wrestlers). Ignoring these tips could cost you your life. Really. Several smart teens have been killed in the US over the last four years by people they met online. Don't become a victim.

2. Bring backup. If you are going to meet, bring a lots of friends (preferably big ones :-)), and someone where you are going. Leave information about the person you are meeting. The bad guys will try and get you to erase the e-mails or bring your laptop or hard drive with you, so they can destroy the evidence. Best case scenario, trust your parents or another adult family member. This has saved more than one teen from being kidnapped, raped or killed.

3. Find your own ride. Don't accept a ride from them or offer a ride to them...even if they appear to be cute and cuddly. Stay in control of where you go and how you are going to get there and back. Bring a cell phone and make sure it's charged. Have others check in on you too.

4. Take it slow. Even if that's not your style, make it your style for any cyberdating situations. Just because they have told you their favorite bands, movies and food doesn't mean you have any idea who they really are. Treat it like a first date. It will feel weird at first. You feel closer than you would on a first date. They will know lots of things about you that you have shared. Often very personal things. But start from scratch. Don't move faster than you are comfortable doing and don't feel pressured. Keep others around for awhile as you get to know each other and trust your instincts.

5. Rat on the Creep! Your parents will kill you if they found out you met someone from the Internet in RL. But if you don't report it to someone, this creep may kill some teen in reality! Most of the time when police arrest an Internet sexual predator, they find lots of e-mails on their computer threatening to call the police if they bothered the teen one more time. Had someone actually called the police, another teen might have been saved. Even if you won't tell your parents, find a way to report the creep. Check out Katiesplace.org for ways you can do that and more safety tips and real stories about real teens.

copyright 2006, Parry Aftab, all rights reserved. For permission to reprint this, contact Parry at Parry@wiredsafety.org.

Appendix D

For Teens:

Finding a Better Faith

A fictional account…

I thought I had met my dream guy. I really did. Now, I see where my mistake was, sure. It was in believing what I saw in the movies and on television. Believing what I read in magazines about true love and soul mates. I believed in the Madison Avenue picture of love, romance and happily ever after, and glossy views of happiness and popularity. I was taught these things my whole life by my everyone I knew and from books, movies, and songs. I was told that if I were good enough, thin enough, charming enough, pretty enough, and exciting enough my life would be fulfilling, happy and exciting. But no one ever tells you how dangerous this blind belief can be.

When I was a freshman in high school, I was miserable. I lived in one of those towns where the same kids are in your grade all the way through school, so everyone gets to know each other pretty well. They knew me in middle school when I had acne and bad clothing and was shy and self-conscious. And then I grew out of that, but no one much noticed. I know I was pretty in the year or two before I died because people started noticing me – people who didn't go to my school, who didn't remember how I used to be awkward.

And it felt good. I felt different and happy and hopeful. I thought to myself that maybe now I would have a boyfriend. Maybe he just couldn't find me before because I was shy and awkward, and it'll definitely happen now that I'm in high school and all the older boys can see how pretty I had become in the last few years. But it didn't. No one looked at me any differently than they ever had and I got depressed. I thought to myself that high school might just be middle school again – that maybe nothing would be different and I would have to go through three more years of being lonely and waiting until something better happened. For a while, I got resigned myself to this fate and then something changed and I got up one morning and said no. I think I said it out loud, actually, it's kind of funny to think of now. I decided that I would say no to this fate – that I wouldn't be alone and I wouldn't be miserable – not anymore. I decided that I would meet someone and I would have a boyfriend within a month or two – do or die – that I would take my life into my own hands. And that I did.

I started going online and searching for people to talk to – people who would be more mature and would understand me. I sorted through people's profiles on Friendster and Xanga.com and set up my own. And then I met someone, and it was just as easy as I ever dreamed it could be. We IMed for hours, about everything and I felt, for the first time, that someone really understood me. Sounds pretty silly now. We talked about our families, our dreams, books that had changed us – everything. I thought I was falling in love. I knew I had found "the one." I was the lucky one, and had found my soul mate early.

When he asked me if I wanted to meet, at first I said no, that I didn't know him well enough. He didn't push it, and instead, we started talking on the phone. He had a very deep voice, which didn't surprise me because he said he was 18, but it probably should have. Anyway, a month later he said he had to meet me. He said he couldn't' stand it anymore – that he loved me – and said that if I wouldn't meet him he would come find me because if he didn't see me he'd die. In the end, it didn't quite work that way, though.

I realized that my parents would kill me if a random guy showed up at the house looking for me. I couldn't have that happen, so I agreed to meet him. It was stupid, I

know, but I was told more time than one that it's okay to do stupid things when you're in love.

I met him at the mall, in the food court. He was 37, not 18. I started crying and told him that he lied to me and I never wanted to see him again. I felt betrayed, and confused. He handed me the rose he had brought and a book of poems. I just stared at them, having problems separating the 18 year old I knew so well, form this man standing in front of me with tears rolling down his cheeks.

While he cried quietly, he told me that he loved me so much – that he knew I would never date him if I knew how old he was, which is true. I worked up the courage to leave. But he started making a big scene – pleading with me not to leave him. Telling me how much he loved and appreciated me, when no one else did. I was afraid someone I knew or who my family knew might see so I agreed – his last request – to go outside to talk.

He said he had a present for me in his car, and could he just give it to me. I said ok, probably the stupidest thing anyone's ever done. He clamped his hand over my mouth so no one could hear the screams. Then he pushed me in his car, throwing a blanket over me and holding me down so no one could see. He poured some smelly chemical over the blanket near my face. At first I held my breath, but finally had to take a breath. I knew I was in trouble, and felt dizzy immediately. I must have passed out. I don't know how long it was before I woke up, and realized this wasn't a horrible dream. It was real. He took me someplace in the woods, dragged me from the car and tied me up. He beat me, while he raped me, crying and telling me he loved me the whole time. I felt like my insides were being ripped out. That was how I lost my virginity. And my innocence. And more.

I still feel like its all my fault. Why did I believe him? Why did I believe that anybody normal could be that into me? Even after all this time, the only answer I can come up with is that I had believed in make-believe. If I hadn't wanted to fall in love so badly, if I hadn't needed someone wanting me to validate how I felt about myself, I wouldn't have let my judgment get clouded. I would probably be alone in my room, depressed, but I'd be better off than I am now.

So believe in happily ever after, but reality too. It's okay to be hopeful because life would be too hard without it. But don't let it cloud your better judgment. Have faith in yourself and don't waste it on people who may or may not love you or save you or complete you. And don't trust people – at least for a while, at least till you know who they really are and what they are capable of. And never just because you talk with them online and on the phone and think you know them. Love and loneliness don't excuse stupid behavior, and they certainly don't buy you another chance to fix it.

I will never know what could have happened in my life – who I could have met or what I might have done, because he killed me before leaving my body for some hikers to find weeks later. I was almost unrecognizable. My parents had to identify me, and the hair, clothes and complexion I worked so hard to make perfect weren't even identifiable anymore. I was ashamed that I had done this to my parents, and my little sister, and most of all to myself.

My friends didn't envy my "kewl" new life. They, instead, mourned me, and even my dearest friends talked about how "stupid" I was.

My little sister couldn't stop sobbing. She held my hand, and clung to the casket when they tried to take it out of the church. I tried to hold her hand back, but nothing happened. I wanted to reach out and comfort her. But from now on, she wouldn't have a big sister to do that anymore. She couldn't climb into my bed and tell me about her kitten and why she wanted to be "just like me" when she grew up.

I hope she wouldn't be just like me. I hope she is smarter than I was, and not as trusting. Not as naive

I wish I had a second chance. I wish I could warn others about this kind of thing. But I can't. I'm dead.

This “love of my life”, my “soul mate” didn’t only rob me of my innocence and any chance at happiness – I’ll never know if I could have made it. I never got a fair shot. If you’re in the same situation I was in, I can’t say if it’ll ever get better, or if you’ll ever be successful, or rich, or pretty, or lose the weight, or get the guy, but I can say you better hang around and try, because I’d do just about anything for the second chance. A chance to find someone real. A chance to know if I could have been happy.

Appendix E

About Teenangels from a school technology director in Wisconsin:

About 5 years ago, I got a phone call from one of the parents in our school district asking that her daughter's Internet and email privileges be revoked. She decided that her daughter would no longer be allowed to be part of the "Cyber World."

When I spoke more with this parent, I learned that the daughter had been harassed online. She had given out personal information and was now receiving inappropriate emails and phone calls at her home.

I immediately looked for resources online to help this family. The Internet is such an incredible resource – I wanted to find a way to convince the family that education regarding Internet use was a better solution than instituting a complete ban for their high school daughter.

As a result of my searches, I happened on information about Parry – I contacted her and she agreed to speak at a school assembly with a parent information meeting to follow. After Parry's talk, I literally had a line of students in my office – these students wanted to help other teens to be safe online. From that group, our TeenAngel chapter was started.

The Teens devoted an entire Spring Break to intensive training and the rest is history. Our TeenAngel chapter works to educate Teens (and parents) about online safety. We have a "Tech" division that works on programming and helps community members with problems ranging from P.C. trouble to instructions on virus removal.

Our teens are highly motivated and highly technologically savvy. Among other things, our group has attended the Wired Kids Summit in Washington D.C. working with legislators and corporate executives to help make the Internet a safer place for kids. One of our teens was featured on "The John Walsh Show" in their "Hometown Hero" segment. Locally, our teens have presented to numerous school, church, and parent groups as well as presented at state conferences focusing on issues relevant to Teens.

This is a great program. In our high school, it has become a place and program for our "Tech" guys to devote their energy and talent.

Appendix F

From Katiesplace.org, written by one of our Teenangels who wants to teach others how to avoid being victimized in the way she had been.

When Your Mentor Becomes Your Tormentor - Alicia's Story

You never notice yourself growing. It's so gradual, so smooth a process that the daily or even monthly changes are simply undetectable. Mirrors don't help – its only in comparing photographs, in seeing yourself at different stages, that one can notice the differences.

My relationship online with Mac grew just that slowly. When we were first introduced online, he was courteous and interested and subtle, none of those childish IMs which are so common, among young teens, flaunting their new-found sexuality like so many new toys. He didn't try to have cyber sex with me, didn't make crude comments or ask me to go on the webcam. It doesn't work like that. He was thoughtful and gentle and nice, and, of course, entirely deceptive, and so we became friends. Just friends. And it was all very innocent - for a time.

It was in the slowest, least noticeable way that he eased me into a more intimate relationship online. He was an expert, but, of course, I didn't know that at the time. The way the conversation moved into more personal territory never felt threatening because it moved so slowly. We would talk for a few minutes more each day, about something a little more personal each day, and some days we could talk about nothing personal at all. He never pushed, never insisted and so convinced me that I wanted to tell him personal things, or 'parrot' those things that he so wanted to hear from me. And I did.

So we talked about everything – not just the sexual stuff. He was interested in me, as a person – my thoughts, my goals, my relationships with friends and family members. He gave me adult advice and always took my side. He was my advocate, unconditionally, at a time in my early teenage life where that was just what I needed. School was: well it was school, mean girls and nasty boys and everyone trying to be all that they're not- And my family and I, were very close, but we didn't always see eye-to eye about everything, sometimes they just seemed to think that I was still a child. But there was always Mac, and I could count on him to see things my way Always online. Always ready to talk. Always on my side. It was the most comforting thing imaginable.

Soon enough, he wasn't just someone that I could trust, he became the someone I needed – I began to believe that he was the only one I could depend on to understand the real me, which is exactly what he wanted, of course. Somehow, in this process, this grooming of me, he had changed me, had destroyed my ability to reason. Imagine, I walked out the door, right out of my own front door into the darkest iciest winter night, with no money and no coat, to meet a madman who I thought was my best friend.

Was I crazy? No. Was I duped? Entirely. When I review it all, comparing my mental photographs of our relationship at different times, I think, how could it have happened? How could my sanity, my reason, my mental state have decayed like that – how did he make me shrink away to nothing? How could I have gone from being a smart, sane girl having casual conversations with an online friend to doing something I would have sworn I could never do –who… shy timid little me?—never!!!!- meeting a total stranger in the dark, cold night – leaving home in the middle of a happy, loving, family holiday meal? My only answer is that I wasn't crazy – I was just under the spell of an incredibly skillful manipulator who knew that slow and steady wins the race – or at least the hearts of young girls. He took me apart and put me back together and bit by bit, day by day, byte by byte, he became the focus of my life and the one who understood me best. Why wouldn't I want to meet someone like that IRL? It felt right.

And yet it was so wrong. The moment he persuaded me into the car, I immediately knew that I was in trouble. I knew. I had this terrible sinking feeling in the pit of my

stomach as we drove down my street, out of my neighborhood, and then, onto the turnpike. Trapped "Quiet" he said. "Let's keep the trunk empty." I kept my eyes cast down, stealing quick furtive glances up at him from the corners of my eyes. Somehow, I instinctively knew that he was like a savage beast, and that I had only to make full eye contact to engage his anger, to force him to attack. I stared down at his shoes as we drove. At his pants, his socks, I studied them, eyes cast down. I could describe it all to you today – that image, that feeling, trapped …it will haunt me forever. Those hours sitting there, the waiting….

What terrible fate awaited me when we arrived at his home? I never envisioned anything as terrible as the reality. When we arrived at his home it was – worse than even I had imagined it could be. It was way worse than a bad after-school movie. It was Friday the 13th and Texas- Chainsaw-Massacre! And he had it planned – days before, maybe months before, maybe the first time we ever spoke. I was stripped, tortured, beaten. …. Raped. Those words still stick to the roof of my mouth and are glued thickly to my tongue. I listened through the windows to cars passing by, to the voices of neighboring families going out for lunch and to the mall and coming home again at night, yet there I remained, collar around my neck, chained to a post, naked. This was me at age 13. Waiting for death. How would he do it? Would he stab me, would I bleed to death, my blood adding yet another stain to the filthy carpet" Would he beat me to death with whips and fists, chained helpless, unable to defend myself?

Into this morbid fantasy, unbidden, a fairy tale that my mother had read to me while tucked warm and safe into my silken little 'blankie' kept flashing into my mind. The one of an Arabian slave girl held captive by her master. The tale unfolds that at the moment her stories ceased to entertain him, to amuse him - then he would kill her, with this in mind, the helpless slave fought for her life with the only weapon she had - her mind... And she became my inspiration. I would persevere, I would not die. My captor would not win this battle. I knew that my family loved me, that they would move heaven and earth to find me. But I had to stay alive until they did. So I struggled, silently, determined to win back the life I had left behind. My life that somehow had seemed to become so empty, so sad… why? I understood now, in those cold hours alone, waiting for the monster's return, it all began to come clear. I wanted my life back! I wanted to feel my mom's gentle kisses good-night and my dad's crushing hugs, I wanted to run outside into the sun, to add my voice to the other happy children's, far, far away from the dark coldness of his dungeon. I wanted to experience anything – anything - except what was happening to me. I desperately wanted to live!

So I waited it out. I prayed. It might not seem, to you, like the most courageous thing to do – I didn't fight him, didn't engage his anger. But, somehow, I knew that he would kill me, throw me away like trash in some cold shallow grave if I resisted anymore. He enjoyed my pain. So, I just wasn't there I left – mentally anyway. This wasn't happening to me. I escaped into my head and tried desperately to hang on to my sanity. It took my whole being to merely breathe. One breath at a time I waited for my death. I knew that one wrong move would cost me my life and so I simply waited, telling myself "today, yeah today they'll find me… rescue me," convincing myself that this would not be how it all ends, that my parents would not find their only daughter's dead and battered body in this evil man's filthy house. I couldn't, I wouldn't, let it end that way. So I resolved to live. Breath by breath. Moment by moment.

And I did. I made it through, a miracle of survival, when so many other girls have been less fortunate. And I can't say if it was faith, or luck, or personal resolve that saved me. And it doesn't really matter. I truly feel that something greater than myself has directed me. I am alive. I was given the second chance that so many others had been denied.

I promised myself in those dark and painful days and endless nights that if I were spared, if I were given a second chance at life, I would share my horror, to teach others -

maybe you - how to avoid becoming his next victim. I would help them understand that the mentor you thought you found online might become the tormenter who steals your heart, your innocence and your faith in mankind. And ultimately, **your life**…..

Mac failed. While the emotional and physical scars may last a lifetime, he didn't shake my faith in myself or in mankind. He may have stolen days, weeks, months, he may have taken my childhood, but the rest of my life is mine. And I have reclaimed it. I will not allow him to torment me anymore. Only I have the power to control my future. I refuse to be defined by his betrayal of my trust, by his cruel sadistic acts or by those dark days, however devastating they may have been. I have a mission and an important role to play. I want to inspire others to move on, past their exploitation, to find their own life mission. I was spared and given a second chance. And I don't intend to waste it. I will continue to speak to young people and dedicate my life to helping catch criminals, like Mac. I am also helping, here, to build KatiesPlace.org and as a volunteer with WiredSafety.org and others.

So, please don't remember me as the girl who was torn, twisted, confused, lured abducted and abused. Remember me for what I will accomplish. Please don't let this tragedy define me. I am so much more than that. And so are you. Join me in this mission. Together we can change the world, one child, and one life at a time. You can read about miraculous rescues and the dedicated and courageous men and woman responsible for bringing victimized children to safety here at KatiesPlace.org. And you can e-mail me through this site. **Please, be safe…be aware…**

MR. WHITFIELD. Thank you, Ms. Sullivan. And Ms. Hahn, you are recognized for 5 minutes. Give her the microphone.

MS. HAHN. It is heavy. Oh well. Thank you for having me this afternoon. As we all know, youth bullying is not a new issue. I am sure, growing up, many of you may have been a bully's victim or at least knew someone who had been called degrading names or in others way been harassed. But bullying is one that can be easily overlooked as kids will be kids.

Bullying has become a universal issue that affects both boys and girls regardless of age or circumstance, and over the past few years has grown in epic proportions, from name-calling and to kids throwing sticks and stones on a playground to invading a person's home via text messaging and the Internet. Thanks to the technologies of today, computer, websites, and cell phones, it has become increasingly easier and more appealing for bullies to seek out victims. Kids who might have been hesitant to participate in bullying in the past can now hide behind an anonymous screen name without fear of being caught.

Name-calling, physical attacks, death threats, these are all things that I have personally gone through. At the age of 12 and a half, I wound up in a state of depression. I am able to be here today and to spread my story across New Jersey because I have gone through years of counseling and was able to recover. Unfortunately, that is not the case for every child. We have kids committing suicide, as most of you know. As a victim of severe bullying both online and off line for years, I fully understand the long-term effects bullying can have on a child. My

bullying experience started with a rumor that quickly escalated into verbal abuse and physical abuse, and eventually on to the Internet. The bullying lasted for almost 6 years of my life. I changed schools, but even that did not stop the bullying, because the bullies found new ways to torment me. For me, the worst part of being bullied was when it was over the Internet, cyber bullying. Because you have no idea who your attackers may be, they can hide behind a screen name, remaining anonymous, while the victims become increasingly vulnerable and defenseless, such as myself. They can say cruel and malicious things, threatening, or even pretend to be other people. Personally, I received instant messages and e-mails saying we are going to kill you, and in detail with what gun, what knife, what they were going to do with my body when they were finished with me. I wouldn't go to the bathroom alone if I were you. You better watch your back. We are going to get you. I am 21 years old now I can honestly say that the scariest thing I have had to face in my life was cyber bullying; and it is something I continue to fear every day I sign on a computer.

So on the Internet, you have no idea who the bully is. I was in class looking at every student as if he or she was the enemy. Because of the bully's mind games, I started having nightmares and couldn't eat. I was physically making myself sick. The bullies got inside my head and made me paranoid, always looking over my shoulder and wondering who the invisible attacker was. After receiving online threats such as we are going to kill you and I wouldn't go to the bathroom, I refused to go to the bathroom while in school. My grades dropped drastically because I couldn't concentrate. I was threatened all the time and afraid to go anywhere by myself. I wouldn't even leave my house without my parents. This continued on and off from sixth grade all throughout high school. Some weeks were quiet and I thought things might be calming down. I would think, well, maybe the bullies got tired of me and moved on to someone new now, as awful as that sounds. But as soon as I got comfortable, the abuse would start all over again.

As hard as I tried, I just couldn't escape the situation. I couldn't run away because there was nowhere to hide. You are probably thinking like most people do and ask me, why didn't you just block the screen name or turn off your computer? Well, I did just that and still the bullying continued. I would block the screen name and in a matter of seconds a new one would be created. Usually the cyber abuse would happen over the weekends, where there was a sleepover or a party, and instead of listening to music or watching a movie, they would sign on the Internet for hours and just create screen names for hours. I would shut off my computer and not go on for weeks at a time. As soon as I would sign back on, the bullying would start all over again.

At first, like many kids do, I tried to ignore the bullies, thinking I was being oversensitive and hoping that by not bringing attention to them, they would just go away. Not only did the bullies not go away, the bullying grew progressively worse and more physical. I was pushed off a school bus onto the concrete and slammed into the glass doors of the school, receiving several concussions. I couldn't hide the bullying anymore and my parents reported every situation to the school. Nothing was being taken care of. When a bully threw sheet metal at my face, my parents then took this issue to the board of education, only to find no records in regards to the bullying I endured. My bullying experience was swept under the carpet. But now with State laws on bullying requiring all schools to have an anti-bullying policy in place and detailing consequences for bullies, that can no longer happen. It is vitally important for victims and parents to know this.

It has always been extremely important to me to get my story out to those who may be facing the same situations I faced in school. Kids need to know that they are not alone and even more importantly, they need to realize that positive things can come out of negative situations. In 2004, I started a Tolerance/Anti-Bullying program, bringing my message into dozens of schools across the State of New Jersey, reaching students from third grade through high school. The program structured around my personal experiences, shows how bullying can affect its victims and their families. The program soon earned the respect of the New Jersey State Attorney General's Office, and in October of 2004, I was asked to be the New Jersey State advocate for the New Jersey Cares About Bullying campaign. As part of the Bias Crime Unit, I speak at State conferences and lectures.

I also work with i-SAFE, as you know, which is a national nonprofit Internet safety organization. i-SAFE teaches safe and responsible Internet use through classroom lesson, through parent programs at home, and through unique peer-to-peer student mentoring. As an i-SAFE mentor, I help teach students how best to avoid becoming a victim of cyber bullying and other online threats, like predators. I teach, among other lessons, the four R's: recognize inappropriate behavior, refuse requests for personal information or a meeting, respond assertively, and report inappropriate online behavior to their parents and their Internet service provider. I also challenge students to become i-MENTORs themselves, which empowers them to spread Internet safety education to their fellow students, their parents and others in their community. There are 234 student mentors in New Jersey alone. Websites like myspace.com are attracting millions and millions of kids. Many log on daily because it is fun to be a part of an online community; however, far too many of them are not aware of the risks or dangers. Rumors and

gossip, whether true or false, are spread around the world instantly. Young children are posting pictures of themselves and they reveal personal information that can lead a cyber predator right to their front door. Schools and parents need to do more to teach students how best to be safe on the Internet.

So far, 45,600 students have been taught i-SAFE lessons in New Jersey schools, but unfortunately, I was not one of those kids. I did not have the benefit of i-SAFE Internet safety lessons in any of the schools I went to before or during the time I was being bullied online. My parents and I were left in the dark about what to do and I suffered greatly. Now, based on my experience with middle and high school students, I know firsthand that Internet safety education works. i-SAFE makes it cool to be cyber safe. i-SAFE's Internet curriculum and community outreach programs connect with kids, enabling them to participate in a fun activity to help them better learn Internet safety lessons. The same with parents. Parents, who often just give up when it comes to computers and technology, learn how to keep their children safe online through i-PARENT boards and instructive parent night presentations.

At the conclusion of my presentations to students and parents, I challenge them to take action, take action to make a difference; take action to become an i-MENTOR; take action to demand that your district use i-SAFE. So in that spirit, I call on Congress to take the same action, take action by passing legislation requiring Internet safety education be taught in all schools so every student will get quality and possible lifesaving education. With that curriculum in place, beginning at an early age, students will learn to take control of their online experiences and be able to recognize and avoid dangerous, destructive and illegal online behavior, and to respond appropriately. Thank you for your time.

[The prepared statement of Samantha Hahn follows:]

PREPARED STATEMENT OF SAMANTHA HAHN, I-MENTOR, I-SAFE AMERICA

Youth bullying is not a new issue. Growing up, many of you may have been a bully's victim or at least known someone who's been called degrading names, or in other ways been harassed. But bullying is something that can be easily overlooked with a *"kids will be kids"* attitude.

Bullying has become a universal issue that affects both boys and girls regardless of age or circumstance and over the past few years has grown in epic proportions, from "name-calling" and throwing "sticks and stones" on the playground to invading a person's home via "text messaging" and the Internet. Thanks to the technologies of today (computers, web sites, and cell phones) it has become increasingly easier and more appealing for bullies to seek out victims. Kids who might have been hesitant to participate in bullying in the past can now hide behind an anonymous screen name without fear of being caught.

Name calling, physical attacks, death threats, nightmares, depression, counseling, and recovery—as a victim of severe bullying both online and offline for years, I fully

understand the long-term effects bullying can have on a child. My bullying experience started with a rumor that quickly escalated into verbal and physical abuse and eventually onto the Internet. The bullying lasted for almost 6 years.

I changed schools three times. But even that did nothing to stop the bullying, because the bullies found new ways to torment me. For me, the worst part of being cyber bullied was on the Internet because you have no idea who your attackers may be. They can hide behind a screen name, remaining anonymous while the victim becomes increasingly vulnerable and defenseless. They can say cruel and malicious things, threaten, or even pretend to be other people. I received instant messages and e-mails saying, "We're going to kill you"; "I wouldn't go to the bathroom alone if I were you"; and "you better watch your back."

So on the Internet, you have no idea who the bully is. You're in class looking at every student as if he or she is the enemy. Because of the bully's mind games, I started having nightmares and couldn't eat. I was physically making myself sick. The bullies got inside my head and made me paranoid, always looking over my shoulder wondering who the invisible attacker was. After receiving online threats such as "We're going to kill you" and "I wouldn't go to the bathroom," I refused to go to the bathroom while in school. My grades dropped drastically because I couldn't concentrate. I was frightened all the time and afraid to go anywhere by myself. This continued on and off from 6th grade all through high school. Some weeks were quiet, and I thought things might be calming down. I would think, "Wow, maybe the bullies got tired of me and moved on to someone new." But as soon as I got comfortable, the abuse would start all over again.

As hard as I tried, I just couldn't escape the situation. I couldn't run away because there was nowhere to hide. You're probably thinking: "Why didn't you just block the screen name or turn off the computer?" Well, I did just that, and still the bullying continued. I would block screen names and in a matter of seconds a new one would be created. I would shut my computer off and not go on for weeks at a time but, as soon as I signed back on, the bullying started all over again.

At first I tried to ignore the bullies by thinking I was being oversensitive and hoping that by *not* bringing attention to them-they would go away. Not only did the bullies NOT go away, the bullying grew progressively worse and more physical. I was pushed off the school bus onto the concrete and slammed into the glass doors of the school, receiving several concussions. I couldn't hide the bullying anymore, my parents reported every situation to the school. Nothing was being taken care of. When a boy threw sheet metal at my face my parents then took the issue to the Board of Education only to find no records in regards to the bullying I endured. My bullying experiences were swept under the carpet, but now with state laws on bullying requiring all schools to have an anti-bullying policy in place and detailing consequences for bullies, that can no longer happen. It is vitally important for victims and parents to know this.

It has always been extremely important for me to get my story out to the ones who may be facing the same situations I faced in school. Kids need to see they are not alone and even more importantly they need to realize that positive things can still come out of bad experiences. In 2004 I started a Tolerance/Anti-Bullying program bringing my message into dozens of schools throughout the state, reaching students from 3rd grade through high school. The program, structured around my personal experiences, shows how bullying can affect its victims and their families. The program soon earned the respect of the New Jersey State Attorney General's Office and in October 2004 I was asked to be the spokesperson on victim's behalf for the state's Anti-bullying Campaign "New Jersey Cares about Bullying." As part of the Bias Crime Unit, I speak at state conferences and lectures.

I also work with i-SAFE, a national non-profit Internet-safety organization. i-SAFE teaches safe and responsible Internet use through classroom lessons, through parent programs at home, and through unique peer-to-peer student mentoring,

As an i-SAFE mentor, I help teach students how best to avoid becoming a victim of a cyber bullying and other online threats, like predators. I teach, among other lessons, the four Rs: recognize inappropriate behavior, refuse requests for personal information or a meeting, respond assertively, and report inappropriate online behavior to their parents and their Internet Service Provider. I also challenge students to become i-MENTORs themselves, which empowers them to spread Internet safety education to their fellow students, their parents and others in their community. There are 234 student mentors in New Jersey alone.

Web sites like myspace.com are attracting millions and millions of kids. Many log on daily because it's fun to be part of an online community. However, far too many of them are not aware of the risks or dangers. Rumors and gossip—whether true or false—are spread around the world instantly. Young children post pictures of themselves, and they reveal personal information that can lead a cyber predator right to their door. Schools and parents need to do more to teach students how best to be safe on the Internet.

So far, 45,600 students have been taught i-SAFE lessons in New Jersey schools. But, unfortunately I was not one of them. I did not have the benefit of i-SAFE Internet safety lessons in any of the schools I went to before or during the time I was being bullied online. My parents and I were left in the dark about what to do, and I suffered greatly. Now based on my experience with middle and high school students, I know first hand that Internet safety education works. i-SAFE makes it cool to be cyber safe. i-SAFE's interactive curriculum and community outreach programs connect with kids, enabling them to participate in a fun activity to help them better learn Internet safety lessons. It's the same with parents. Parents, who often just give up when it comes to computers and technology, learn how to keep their children safe online through
i-PARENT Boards and instructive Parent Night presentations.

At the conclusion of my presentations to students and parents, I challenge them to take action. Take action to make a difference, take action and become an i-MENTOR. Take action and demand that your district use i-SAFE. So in that spirit, I call on Congress to take action. Take action by passing legislation requiring Internet safety education be taught in all schools, so every student will get a quality and possible life saving education. With that curriculum in place beginning at an early age, students will learn to take control of their online experiences and be able to recognize and avoid dangerous, destructive and illegal online behavior, and to respond appropriately. Thank you.

MR. WHITFIELD. Thank you, Ms. Hahn. Well, Mr. Livingston and Mr. Herrera, what about her suggestion that Internet safety be a required course for students?

MR. LIVINGSTON. I think that makes an enormous amount of sense and that is what our trainings are going to be about and incorporating that into the--infuse it into the regular curriculum, where they are doing instruction on bullying and harassment.

MR. WHITFIELD. Is bullying a real issue in the schools today?

MR. LIVINGSTON. Yes, a tremendous issue. And in fact, Mr. Herrera has a survey of students that was done at the Somerset High School. And in each question regarding bullying, it is a clear problem students indicate, maybe 150, 200 students, I think, were surveyed on this--indicates that they many times don't report it. Many times they are bullied. Many times they don't know what to do about it. And sort of

some of this survey gives you a reflection of the helplessness, a feeling of helplessness.

MR. WHITFIELD. Well, Ms. Hahn talked about cyber bullying, but I suppose there are all sorts of bullying, right?

MR. LIVINGSTON. Yes, yes.

MR. WHITFIELD. Could you give me some examples of what you all have experienced, Mr. Herrera, in your school?

MR. HERRERA. Yes. Right now the Somerset County Vocational and Technical High School is following the oldest bullying prevention program, which was created by Dan Olweus in Norway. And the program is the core elements. What we did, we assessed our school needs through a questionnaire. We have an antiviolence evaluation response team currently in place. That is our school-base linkages program, and we identify and we prevent. We are a therapeutic, proactive community. We have ongoing in-service to teachers. We have the State Police come in and we decided to focus on the instructors who have the most contact and could identify students in need that are being bullied and harassed.

We increase supervision and supervision and supervision. And the challenge that we are facing now as school administrators is when the bullying and harassment occurs outside the school, and what are we going to do to address that? As school administrators, we are charged with responsibility and we can discipline students if it impacts the school environment. Outside of the school, we need the continued cooperation that we have with the various local and State agencies.

MR. WHITFIELD. Do you feel like you have the discipline tools that you need? I mean, a lot of administrators of schools I talk to today sound like they are almost afraid to provide much discipline.

MR. HERRERA. I believe that right now we do. We also focus on the therapeutic and the rehabilitation of positive psycho-emotional growth of the students, so we target that in addition to the punitive, the educational, and the therapeutic.

MR. WHITFIELD. And what is the relationship between bullying and child pornography?

MR. HERRERA. I think it starts off with harassment and I think the three-pronged--the bullies, then you have the victims. We do a lot of assertiveness training with our students, also, which I think is very, very important. And also the bystanders. The organization that Mrs. Aftab, which we will be investigating after today, is the peer-to-peer in a positive relationship, besides the meaningful conversations that students have with our instructors or faculty, but also with each other. So we are going to definitely be research--

MR. WHITFIELD. Do you want to comment on that, Ms. Aftab?

MS. AFTAB. Yes, if I may. Thank you, Mr. Chairman. Our specific on site on cyber bullying is tostopcyberbullying.org, and the connection--to respond to your question, the connection between child pornography and cyber bullying is that cell phones that have photo capability and digital cameras are being used by cyber bullies to torment each other in sexual ways. Kids that are at a slumber party, there is a kid they don't like, they wait until she is getting undressed and take her picture. Dressing rooms, locker rooms, bathrooms are being used to take pictures of kids. Up-skirt pictures are being taken with all kinds of different mechanics, a shopping bag, a purse opened to go next to somebody who has got a short skirt. These are then published on the Internet. They are all child pornography. They are also incredibly, incredibly humiliating.

We also have cases where--young people are not known for great judgment and a young girl may like a boy, and we had a case in Westchester, New York, where a girl liked a boy, so she took a video of herself in mock performance of oral sex and she sent it to the boy she liked, thinking that that would intrigue him into dating her. It didn't and he shared it with his 100 best and dearest friends and it is all over the Internet. So this is a real issue.

In addition, you had asked a question about schools. One of the big problems we have is a constitutional issue with public schools. So cyber bullying typically happens, the actual act of posting it happens from home, from a cell phone outside of school premises after school hours, not using school equipment, not a school-sanctioned event. And right now, constitutionally, the cases have held that if the school takes action during school, so that in a situation like this one, not on the in person bullying, if something was posted from a slumber party that affected her and the school takes action, the schools are sued and they generally lose that lawsuit and it costs them $50,000 or $60,000. That has happened here in New Jersey frequently. Actually here in Warren Township, it was one of the first cases where criminal charges were brought against a cyber bully for taking these actions. So it is a real challenge. We have a risk management program, and the program out of Norway is the best bullying program, and there was actually Federal money that was given to a sheriff in Ohio and we will be working with him on dovetailing our cyber bullying program with the Norwegian program. So we will give you everything you need.

MR. WHITFIELD. Okay. Ms. Hahn, are you still an advocate in the Attorney General's Office?

MS. HAHN. Yes, I am.

MR. WHITFIELD. And could you briefly explain the responsibilities in that position now?

MS. HAHN. At all the State-wide cyber bullying conferences, I speak on victims impact and I share my story for the educators that appear, and the law enforcement there. And occasionally, very far and few between, I have gone to law enforcement training sessions where, there too, I share my story.

MR. WHITFIELD. And you are finding that a lot of students have experienced this same bullying that you have, I am assuming.

MS. HAHN. Yes. At first it was very difficult for me, because I didn't realize how many kids are going through experiences exactly like mine. Some students, yes, not as severe. Others, exactly like mine or more so. They, like myself, are having thoughts of suicide and why am I alive, and my teachers aren't doing anything. I am going to faculty asking for help, and I went to my guidance counselor and they laughed at me, and this is a really big problem, especially knowing that there is a State law in effect. It is happening all over and I think, with going into the whole cyber bullying and everything, I think the older generation, parents, we have mentioned a couple of times that we live in a generation where kids have their own cell phone with the picture phones and their own computers or laptops in their own rooms. The door closes. Parents, mom and dad don't know what is going on. They don't know if their child is the bully or the victim. Private schools now are requiring every student to have a laptop to travel class to class. It is awful. I know, in 2003, when the anti-bullying law was first passed, schools were giving classes and lessons and there were conferences and correctional officers were going through training. I have spoken to many, many faculties and they say that since then, there really haven't been any training programs and that it is something that they want, especially Internet safety.

MR. WHITFIELD. Well, thank you for the great job you are doing. And Ms. Sullivan, you, of course, testified in Washington, but tell me again how long you have been a Teenangel?

MS. SULLIVAN. For about 2 years now.

MR. WHITFIELD. And you have spoken to how many different schools during that time?

MS. SULLIVAN. I graduated from my grammar school, so I went to my high school and I have spoken to them and some other schools in my area.

MR. WHITFIELD. Right.

MS. AFTAB. And about Teen People.

MS. SULLIVAN. Oh. And then, I was honored by Teen People, as I said, when I was in Washington.

MR. WHITFIELD. Right. Well, we appreciate the great job that your organization is doing, and we look forward to working with you. At this time, I will recognize Mr. Ferguson.

MR. FERGUSON. I look forward to meeting Spiderman. I was born in Bergen County and it ain't cheap there, either. But first let me thank each of the five of you for being here. Each of you in your different ways is having a really positive impact on different aspects of a problem which we are learning more and more about. And it is disturbing, it is upsetting, and I know--I mean, I speak as a former teacher, I speak as a legislator, but I also speak as a parent, and the work that you are doing is extraordinarily important in different ways, by raising people's awareness, encouraging people to learn more about the problems that some of this technology is raising. We know that technology brings so much good and so many opportunities for good, but it is a double-edged sword and it brings incredible opportunities for people to do bad things too, and that is what this is about. This is about--our investigation into this is about learning about what you all are doing on the frontlines and about how we can multiply the good efforts that you are doing to try and make other people aware of them. So first, let me thank you for that, and I know, Mr. Chairman, we are bumping up against our time constraints here, but I really wanted to get that out first and foremost, to thank you for testifying in front of our subcommittee and for the work that you are doing in the field and in your various areas.

Mr. Livingston, could I just ask you about your district's interaction with some of these social networking sites? Has the district had any contact with some of the direct networking sites, or the social networking sites, to express some concerns that you have had about some of what goes on here?

MR. LIVINGSTON. Not to my knowledge. They have had connections of concern among themselves and concerns about getting out the word and the message, and that is another reason now. The concerns have raised to such a level at this point that we are doing this training in the fall to bring up to, I think, some need to have this information. I think they need to hear what we are hearing today, the kinds of testimony you are hearing today, so they can bring it back and put it on the priorities. As you know, in schools, there are a million priorities. Everything is a priority. Everything is a mandate. And I think that kind of training will help to bring it to conscious level--more work on this and more training in terms of the students, getting to the students and the teachers.

MR. FERGUSON. Would you comment on that briefly, if you would like?

MS. AFTAB. Certainly. As you know, we have been inside all of the major social networks for the last year and a half. We started with MySpace when they were a twinkle in Tom's eye. It had six million users in February a year ago, 2005. At our request, they created a special

e-mail address and people to work with schools at schools at--it is either school or schools@myspace.com. They are issues. I am testifying tomorrow in Washington and you will hear more, and tomorrow we will be announcing a seal program. People have been yelling at us. They said that if I am an Internet privacy and security lawyer, I should take my expertise to work and help WiredSafety come up with a way of spotting the social networks who are doing a better job, who care more, who are implementing best practices, caring about kids' privacy in the various settings, and you will be able to spot them because it will have our seal on the front of the page. So we will be talking about that tomorrow a little bit more.

It is a huge challenge and as the superintendent had testified, schools have these standards now, the No Child Left Behind. Schools don't have time to implement Internet safety programs as a stand alone, because then something else is going to fall aside. So we have our new curriculum that you will be hearing about in the next month and a half. It launches in September. Totally free. It builds into everything you are doing scholastically. It is put together by Art Walinski, who you know, from New Jersey, part of the 21st Century Program. A real simple, short thing that will teach kids and adults about cyber bullying and especially about responsible use of social networks. So in little sneaky ways you have one from column A, two from column B. You have to come up with all of these little things that will work. And the social network challenge has changed the playing field. I don't sleep anymore. Unfortunately, it hasn't affected my eating patterns. But we have to do something and our tag line--Ellen, do you have the one about the more information you give your kids? We have two things that we are going to be launching and this is--well, I will be showing one tomorrow that is an animation, but this was put together on social networks and it is a print PSA, and that is it, and it is the more information you give your kids, the less information they will give a stranger. And I can't train parents to teach their kids about Internet safety. I can teach them to talk to their kids and give them little snippets as part of our Take Back the Net initiative. Well, you will hear about that--it is time. And we now have the Mothers Against Internet Sexual Exploitation that will be announced, that was put together because of your hearings. Women, mothers come to me and say, we need to do something, so we are.

MR. WHITFIELD. Thank you.

MR. FERGUSON. Mr. Chairman, I am just very pleased to have this panel and our previous panels. I am very pleased that you brought this subcommittee's hearing to our district here in New Jersey. I am honored that you are here and very much appreciate your work and our staff's

work in putting this day together. I think it has been enormously instructive and I appreciate it and I yield back.

MR. WHITFIELD. Well, thank you very much for your continued leadership, Congressman Ferguson. And we have enjoyed being in New Jersey very much, and I want to thank all of the panels, and I would remind you that we do read all of the opening statements. I don't read all of them, the staff reads all of them and we use that information to go into other areas. So we genuinely thank you for your time in preparing the opening statements as well as being here and giving the opening statements, and for your continued leadership. And we are always open to suggestions that you might have. So thank you very much. We have really benefited from this and look forward to working with you and look forward to seeing you in Washington tomorrow.

MS. AFTAB. Thank you.

MR. WHITFIELD. And with that, the hearing is adjourned.

[Whereupon, at 1:25 p.m., the subcommittee was adjourned.]

○