AUTHENTICATED
U.S. GOVERNMENT
INFORMATION
GPO

CHATTING ON-LINE: A DANGEROUS PROPOSITION FOR CHILDREN

HEARING

BEFORE THE

SUBCOMMITTEE ON TELECOMMUNICATIONS AND THE INTERNET

OF THE

COMMITTEE ON ENERGY AND COMMERCE

HOUSE OF REPRESENTATIVES

ONE HUNDRED SEVENTH CONGRESS

SECOND SESSION

MAY 13, 2002

Serial No. 107–102

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

80–669PS WASHINGTON : 2002

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

W.J. "BILLY" TAUZIN, Louisiana, *Chairman*

MICHAEL BILIRAKIS, Florida
JOE BARTON, Texas
FRED UPTON, Michigan
CLIFF STEARNS, Florida
PAUL E. GILLMOR, Ohio
JAMES C. GREENWOOD, Pennsylvania
CHRISTOPHER COX, California
NATHAN DEAL, Georgia
RICHARD BURR, North Carolina
ED WHITFIELD, Kentucky
GREG GANSKE, Iowa
CHARLIE NORWOOD, Georgia
BARBARA CUBIN, Wyoming
JOHN SHIMKUS, Illinois
HEATHER WILSON, New Mexico
JOHN B. SHADEGG, Arizona
CHARLES "CHIP" PICKERING, Mississippi
VITO FOSSELLA, New York
ROY BLUNT, Missouri
TOM DAVIS, Virginia
ED BRYANT, Tennessee
ROBERT L. EHRLICH, Jr., Maryland
STEVE BUYER, Indiana
GEORGE RADANOVICH, California
CHARLES F. BASS, New Hampshire
JOSEPH R. PITTS, Pennsylvania
MARY BONO, California
GREG WALDEN, Oregon
LEE TERRY, Nebraska
ERNIE FLETCHER, Kentucky
JOHN D. DINGELL, Michigan
HENRY A. WAXMAN, California
EDWARD J. MARKEY, Massachusetts
RALPH M. HALL, Texas
RICK BOUCHER, Virginia
EDOLPHUS TOWNS, New York
FRANK PALLONE, Jr., New Jersey
SHERROD BROWN, Ohio
BART GORDON, Tennessee
PETER DEUTSCH, Florida
BOBBY L. RUSH, Illinois
ANNA G. ESHOO, California
BART STUPAK, Michigan
ELIOT L. ENGEL, New York
TOM SAWYER, Ohio
ALBERT R. WYNN, Maryland
GENE GREEN, Texas
KAREN MCCARTHY, Missouri
TED STRICKLAND, Ohio
DIANA DEGETTE, Colorado
THOMAS M. BARRETT, Wisconsin
BILL LUTHER, Minnesota
LOIS CAPPS, California
MICHAEL F. DOYLE, Pennsylvania
CHRISTOPHER JOHN, Louisiana
JANE HARMAN, California

DAVID V. MARVENTANO, *Staff Director*
JAMES D. BARNETTE, *General Counsel*
REID P.F. STUNTZ, *Minority Staff Director and Chief Counsel*

SUBCOMMITTEE ON TELECOMMUNICATIONS AND THE INTERNET

FRED UPTON, Michigan, *Chairman*

MICHAEL BILIRAKIS, Florida
JOE BARTON, Texas
CLIFF STEARNS, Florida
Vice Chairman
PAUL E. GILLMOR, Ohio
CHRISTOPHER COX, California
NATHAN DEAL, Georgia
BARBARA CUBIN, Wyoming
JOHN SHIMKUS, Illinois
HEATHER WILSON, New Mexico
CHARLES "CHIP" PICKERING, Mississippi
VITO FOSSELLA, New York
ROY BLUNT, Missouri
TOM DAVIS, Virginia
ROBERT L. EHRLICH, Jr., Maryland
CHARLES F. BASS, New Hampshire
LEE TERRY, Nebraska
W.J. "BILLY" TAUZIN, Louisiana
(Ex Officio)
EDWARD J. MARKEY, Massachusetts
BART GORDON, Tennessee
BOBBY L. RUSH, Illinois
ANNA G. ESHOO, California
ELIOT L. ENGEL, New York
GENE GREEN, Texas
KAREN MCCARTHY, Missouri
BILL LUTHER, Minnesota
BART STUPAK, Michigan
DIANA DEGETTE, Colorado
JANE HARMAN, California
RICK BOUCHER, Virginia
SHERROD BROWN, Ohio
TOM SAWYER, Ohio
JOHN D. DINGELL, Michigan,
(Ex Officio)

CONTENTS

CHATTING ON-LINE: A DANGEROUS PROPOSITION FOR CHILDREN

MONDAY, MAY 13, 2002

HOUSE OF REPRESENTATIVES,
COMMITTEE ON ENERGY AND COMMERCE,
SUBCOMMITTEE ON TELECOMMUNICATIONS AND THE INTERNET,
Oshtemo, MI.

The subcommittee met, pursuant to notice, at 1 p.m., in the Kalamazoo Valley Community College M-Tec Facility in Oshtemo, Michigan, Hon. Fred Upton (chairman) presiding.

Members present: Representatives Upton and Bass.

Staff present: Kelly Zerzan, majority counsel; Will Nordwind, policy coordinator/counsel; Hollyn Kidd, legislative clerk; and Brendan Kelsay, minority professional staff.

Mr. UPTON. Good afternoon everyone. I want to welcome everyone to KVCC's wonderful M-Tec facility for this field hearing of the Telecommunications and Internet Subcommittee entitled Chatting On-Line: A Dangerous Proposition for Children.

I want to pay particular thanks to Dr. Marilyn Schlack and Bruce Koper for making sure that everything worked out terrific in having us here today.

As the subcommittee chairman and parent of two young children who use the Internet at home for both school, work and fun, there are few issues that are more important than making sure that our kids are protected on-line. I felt it was vitally important to hold this hearing not in Washington DC, but in Kalamazoo to help spread the word to the families of Southwest Michigan that sadly we are not immune from the ugly underside of chat rooms and that we can and must fight back against those on-line sexual predators who seek to sneak into our homes via the home computer and do harm to our kids.

When a person comes to your door and knocks on it, you can teach your kids to look out the window or through the peephole and see who it is before they decide whether or not to unlock the door and let that individual in. You teach them never to open the door to a stranger.

Also you can always teach your kids not to talk to strangers outside in the street. But in this age of home computers and the Internet, parents do not necessarily have that luxury or security anymore. Pedophiles and sexual predators have figured that out and they have made chat rooms their latest stalking ground.

Alarmingly, national surveys suggest that 1 in 5, 20 percent, of young Internet users have received an unwanted sexual solicitation

via on-line chat rooms. In the Southwest Michigan area alone, we have had a number of tragic examples.

A 21 year old college student has been accused of having sex with three Richmond girls, a 14 year old and two 13 year olds, whom he met on-line.

A 23 year old Oregon man pled guilty to crossing State lines to have sex with a 13 year old girl from Kalamazoo; they met in a chat room.

A 34 year old Brooklyn man, who claimed to be a 17 year old boy, was sentenced last August for having sex with a 14 year old girl from Michiwauke. They met on-line, traded photos of each other, and had conversations about sex.

These are but a few examples of how evil sexual predators are preying on our communities and we know there are many more.

Today we will hear from a number of witnesses including Katie Tarbox, a young woman who has the courage to step forward to tell her terrifying story of how, when she was in her early teens, she was preyed upon by an adult who used a chat room to take advantage of her. She is telling her story so that parents and children in Southwest Michigan can learn lessons from her experiences and hopefully avoid such dangers on-line.

She is to be commended for her courage and I know that this is not easy for her.

We will also hear from John Karraker, father of a Kalamazoo teenager, who was also preyed upon by an adult on-line. John is stepping forward today to provide his perspective in hopes of helping other fathers and mothers protect their kids.

He is not only a father, but also a Public Safety Officer here in Kalamazoo. He knows that if it can happen in the house of a Public Safety Officer, it can happen in any house.

He is testifying today solely in his capacity as a dad. Given that he courageously puts his life on the line in the service of our community every single day, it should come as no surprise that he is using his off-duty time to be with us today to help our community protect kids on-line.

Other witnesses include Mr. Jim Gregart, Kalamazoo County's outstanding prosecuting attorney; Ruben Rodriguez of the National Center for Missing and Exploited Children; Caroline Curtin of America Online, which offers a number of parental controls like kids-only chat rooms; and Kathleen Tucker of I-SAFE, a non-profit organization dedicated to educating kids about on-line safety.

I really want to thank all of our out-of-town witnesses for traveling great distances to be with us today.

I have voted for and Congress has passed several laws in an attempt to protect kids from some dangers on-line. Unfortunately, the Supreme Court recently struck down one of those laws which banned virtual child pornography. Virtual child pornography looks just like the real stuff, but it is generated by a computer.

However, I am an original co-sponsor of a measure that rewrites the law to pass constitutional muster in light of the Court's ruling. I understand that the House will have this legislation up on the House floor next week.

The Court's decision follows on the heels of the Court's 1997 decision to strike down those portions of the Communications Decency

Act which had made it illegal to send pornography to children via the Internet. Still pending in the courts is the Children's Internet Protection Act, which requires schools and libraries that receive Federal funding to employ Internet filtering software and have written Internet safety policies to protect children from indecent material.

Let us hope for a comeback in the Courts.

But even those laws did not address the problem of protecting kids from the dangers of chatting on-line. Getting into one of those chat rooms is easier than getting on a bike, but I would argue that it is much more dangerous.

I introduced a bill, which was recently approved by our subcommittee, which would set up a child/family space on the Internet known as dot-kids. Just like we have dot-com and dot-org, we will have dot-kids. It will be in essence like a children's section of the library, where parents could send their kids to be safe on-line.

Chat rooms would be banned in the dot-kids space unless they were specifically designed and operated to protect children from harm, and the content in the chat room is both suitable for children under 13 and not harmful to them.

I expect this Bill to be on the House floor for vote next week as well.

However, even with all of these measures, the bottom line is that there is no better protection from on-line dangers than proper parental supervision. This means that we, as parents, need to become better aware of the dangers and how to avoid them. Then we must also teach our kids.

So today's hearing is designed to help us accomplish this mission around the country, particularly here in Southwest Michigan.

I also want to welcome a friend and dad, Congressman Charlie Bass, to Kalamazoo. He is a member of this subcommittee from New Hampshire. He has traveled a great distance to be with us. He cares deeply about the issue.

With that, I recognize my friend and colleague, Mr. Bass.

Mr. BASS. I thank you, Mr. Chairman, and I would like to associate myself with your remarks which were right on mark.

This hearing is taking place here in Michigan, but it could easily take place in any community anywhere in the country, including anywhere in my district, anywhere where children can have access to the Internet and communicate.

Like all communication issues, I have discovered that they are so complex that there are never any clearly definable issues or solutions. One has to examine First Amendment rights and the ability to communicate. One has to look at the issues of the fact that the Internet is really one of the greatest technological inventions of the late 20th, early 21st century which will probably keep America ahead for many, many decades to come.

However, as my friend from Michigan here mentioned, there are some very dark and unpleasant sides to this new technology, most notably the issue that we are discussing here today.

It is my hope that we can discuss issues, such as whether or not the criminal justice system is adequately prepared to be responsive and to deal with what will undoubtedly be a growing problem in society; what efforts are underway to teach and prepare children

to deal with chat rooms, especially children that may not understand the implications of the types of discussions and the motives of sexual predators when they get in a chat room environment; and most importantly, the issue of how communities and parents deal with children that are exposed to this kind of environment.

I had the pleasure of having lunch with Katie before we appeared here today, and she was kind enough to give me a copy of her book to read, which I will. I believe in this book one of the issues that is discussed is how she was ostracized by her own community and her own friends and other parents after this event occurred.

I know that is not strictly within the jurisdiction of this subcommittee, but I think that it is something that all of us need to think about carefully because we are not going to move forward and deal with this issue until we, as society, are willing to accept the fact that it can happen to anybody, in Michigan or New Hampshire or anywhere else in the country.

And there may be policy solutions, but as Congressman Upton said, it is parents, families, and communities that bear the ultimate responsibility for solving and dealing with these problems.

With that, I yield back, Mr. Chairman.

Mr. UPTON. Thank you very much.

Our first witness is Ms. Katie Tarbox.

Katie, the time is yours.

STATEMENTS OF KATHERINE TARBOX, NEW CANAAN, CONNECTICUT; ACCOMPANIED BY JOHN KARRAKER, KALAMAZOO, MICHIGAN; JAMES J. GREGART, KALAMAZOO COUNTY PROSECUTING ATTORNEY; RUBEN D. RODRIGUEZ, DIRECTOR, EXPLOITED CHILDREN UNIT, NATIONAL CENTER FOR MISSING AND EXPLOITED CHILDREN; CAROLINE CURTIN, DIRECTOR, INTEGRITY ASSURANCE, AOL, INC.; AND KATHLEEN TUCKER, DIRECTOR, I-SAFE AMERICA, INC.

Ms. TARBOX. Thank you, Chairman Upton, for inviting me here before the House Subcommittee on Telecommunications and the Internet, and thank you, Congressman Bass.

I am very pleased to be here today. I am only 20 years old and I have to say that when I first began this fight, as I will call it, in trying to help the education regarding Internet dangers, this has always been one of my goals. I am happy to be here encouraging legislation and whatnot. I believe it is the right step and going in the right direction.

I have probably told my story now over 200 times. I go around the country speaking and I have sometimes written it out, but I always feel that the best way to tell my story is just by telling it raw. People can read my written testimony, but even though this happened 7 years ago, I want people to see that there are raw emotions and that this did deeply affect me and my family and my community.

I was thirteen years old when I first started using the Internet. My family received the free CD-ROM of hours from America Online, and back in 1995, there was not much press or news regarding the Internet.

We knew that we were one of the first families in the country to sign up for the Internet. I had some idea about what a modem was, but I did not really understand what it was. I just knew that it made some funny noises and that it could connect me to millions of other people in the country.

My family thought that we were signing up for the Internet to buy airplane tickets, and my sister was going to do a college search. Perhaps we could shop, and, you know, we could go into chat rooms.

I had learned about the Internet at school. We were doing an Everglades project connected with CNN and we were connected with other classrooms. The way that we had used the Internet was that we would go into chat rooms to talk to other kids about what they were doing.

So my introduction to the Internet was that this was a place where you go on the computer, and you would meet people and you would go into chat rooms. Quite honestly, I thought that was all that America Online had to offer me because it was the thing that was most boldly advertised when you would sign on.

I started going into teen chat rooms. I did not use them that much, maybe about an hour a day. I was a very active kid. I was a high honors student. I was a national swimmer. I played piano. I was in my select chorus at school, and one of the things that the Internet offered me was that, while I was pretty busy, if I could not call my friends at 11 o'clock at night, I could go on the Internet and my parents thought that it was a great thing. You know, I could go and talk to other kids, maybe from Florida about swimming, or I could talk to them about music.

At times I found it discouraging. There was a lot of heavy sexual remarks, but I kept on signing on hoping, you know, maybe there would be someone out there that I could talk to.

It was a September Sunday morning that I signed on and I asked if anyone wanted to talk to a 13 year old female. I immediately got a response from 23 year old Mark. And I sat at my computer and I thought, "Oh, no, I cannot talk to somebody this old."

I was hesitant to reply, but sitting there I thought, "Well, this is never going to leave the Internet. It is never going to go beyond this."

And so I replied back. He started to ask me a few questions about where I liked to shop and what bands I liked. And I really liked Dave Matthews Band at the time and he had gone to concerts. He could tell me about the lead guitarist; he could tell me about the singers, he could tell me about the songs. And we started to have conversations.

We talked about places we had both gone and I honestly never thought that I would have anything in common with an adult, but this had proved me wrong. In my 13 year old mind, I thought, "Wow, this is fate. I mean we have met on the Internet. This connection, you know, is rare, and we have all these things in common."

And he was intelligent. And I think that was the thing that most attracted me to him. At 13, you think that you are a little bit more mature than the rest of your classmates at school, or you think

that you know it all, and so I was definitely attracted to something like this.

I did not think of it as a romantic relationship, but I wanted to see what could happen. I was not really sure. I did not think that any 23 year old guy would have much of an interest in a 13 year old girl.

Over the next couple of months, we began corresponding via E-mail, the telephone. My parents did not know about this, and I did not tell my friends. I thought that they would pass it off as this is sexual. "Katie, this is not a good idea. All he wants you as, he just wants you for sex," and this clearly was not.

We never once talked about sex or anything romantic really. I thought he was a positive influence in my life. We actually talked about politics. There was a Presidential election that year, and we talked about the different campaigns, and he really made me feel mature. He really made me feel like I was someone special.

And at 13 when you are trying to deal with issues of confidence and you are trying to find an identity, this made me feel just, oh, so special.

He became my world; he became my best friend. He told me that I was beautiful, told me I was smart; he told me all the things that I thought I needed to hear at that age. And, yes, I did hear this from my parents, but my parents are not an older guy. And, a 13 year old girl, I think that anyone who has been in that position can understand what kind of value you would place on that type of attention.

He kept on pressuring me to meet him and I was always hesitant. I did not know how that could happen. I was from Connecticut; he was from California. And I did not expect that I was going to invite him over to my house. I did not expect that I was going to go to California.

While I did want to meet him, I just was not sure about logistically how it would work out. He once again suggested more meeting times. I tried to offer up that I was very busy, and in fact that I was going to Texas the next week for a national swim meet. He said, "Well, why don't I come?"

And before I could say no, I said yes. I think it was my emotional side taking over and just felt that I really did want to meet him.

I was not sure what was going to happen. I did not know if he would come to the swim meet and watch me. But nonetheless, I did tell him where I was saying. And I was always so excited about seeing him that I never really thought I am meeting an older man off the Internet.

I flew to Dallas, Texas, with my swim team, and my mother was a chaperon. And I was just so, so excited about seeing him. I went to dinner. He was supposed to arrive about 7:30 and he did not come. And I was a little disappointed that he was not there, so I went to bed.

And then at 9:30 I got a call from him. I was staying with my swim mate, and he said he was there. I had told this swim mate, because she was a good friend of mine, about this relationship, and she once again said, "Oh, he just wants you for sex." And that confirmed for me that, you know, I could handle this relationship. I was mature, I was responsible, this is different.

She held herself against the door and said, "No, you are not going to see him."

And I said, "No, I am." I told her the room number where I would be going to and pushed her to the side.

I know the scariest part to all of this was that I never thought that I was putting myself in a compromising situation. I never thought that I could be killed or raped. I never thought that Mark would be any other person than he said he was. I was always telling the truth about who I was and you trust so much.

You are told to trust adults. And I did not think that anything dangerous could happen. I really felt like I knew this person.

We had exchanged pictures, but his were from so far away that, you know, I could not make out any distinguishing features or details.

I knocked on the door and opened it up, and I immediately saw an adult. I thought, "Oh, my gosh, this is an adult," and I became very uncomfortable.

I knew that he was an adult. I knew he was older. But over the Internet you buildup so much fantasy that reality does not have to be accepted. That was one of the things that I liked about the Internet, was that nobody judged me on it because they did not have reality right there.

He invited me into the room, and I felt uncomfortable. He was trying to do anything he could to make me feel at ease. He started to talk about his flight. He missed his connection, and then he took me to the bathroom to show me that there was no soap dish.

Then he tried to compliment things about my physical appearance like my hair, anything he could do to make physical contact. He sat me down. And it had been about a half and hour, and I thought, "Well, okay. I should say goodbye and, you know, maybe we will meet tomorrow."

So I sat down on the sofa, was ready to say goodbye, and then he wanted to read my palm and tried to drag things out. I allowed him to read my palm; he told me I was going to have a rich and successful life. And then he looked away and he said, "Katie, I have been thinking about you all day and I have been thinking about doing this."

He leaned over; he kissed me, groped me, and essentially I was molested.

I always thought that if I would be in a situation where I was receiving unwanted sexual advances that I would transform into Wonder Woman or I would, you know, be this strong person, especially because I come from a family of very strong women.

Watching the DARE videos in my class at school, I thought those girls are so stupid. They should just fight back. But I realized in that moment you become so confused.

I became completely numb and passive. I thought, "Do I owe this to him? Of course, he did not come all the way from California just to have a talk."

I was very disappointed in myself and overwhelmingly I felt very dirty for what was happening. I felt that I had lost most of my innocence in those 10 minutes or so.

There was a knock on the door, and I knew it was my mother. It was one of those things. Of course, I did not tell my mother about this relationship, but it was my gut telling me it was her.

And it was her. She had gathered hotel police and security and come up and gotten me. My friend, who I was staying with, had told my mother. I felt very embarrassed and disappointed.

And while I did feel relieved that I was saved, the feelings of disappointment and embarrassment dominated.

I was taken upstairs and I was interviewed by the police. I wanted this all to go away. I did not want police interviewing me and whatnot. So I knew that if I denied that anything sexual had happened, this would go away.

So I said that I had met him over the Internet. We had met there, but nothing had happened. Then they came back and said, "We have been talking to him for about 10 minutes and his name is not Mark, but it is really Frank Kufrovich. And he is not 23, but 41."

They told me he was from California and that he was actually a wealthy financial advisor from the area.

I thought to myself, "Who in the hell had I been talking to for all this time?" And yet the feelings that I had for Mark and this friendship that had progressed, I did not want to admit to myself that he had been lying to me all this time. And I felt very saddened by the fact that I was not going to be able to talk to him anymore.

I went home. And the hardest part to all of this was going home. Everyone thinks that it would probably be those 10 minutes in the hotel room, but no.

I come from a community where something like this would probably be hidden. You probably would not talk about this; it would probably be one of those skeletons in the closet. But because this happened with my swim team there, it was all known, and girls wanted to share these rumors.

So it went around my school that I was pregnant with his child and that I had given myself an abortion with a coat hanger in the bathroom, just horrible, horrible rumors. I was at the top of the class and now to be labeled as a slut or, you know, promiscuous, this was very difficult.

I did not talk about it. I lost all of my friends. Parents in the town thought, "Well, you know, she went to go meet him. Of course she is asking for it."

And parents were afraid that Frank would fly up from California and hurt their children. So I became like the Lolita of the town. I lost all my friends. It was a very alone and empty period.

Ironically, I had lost my best friend already, who was Mark, and then I lost all my other friends.

On top of that, I had parents who were trying to regularly shuffle me to psychologists because they thought, "Well, if she is going to meet somebody off the Internet, then she must be crazy."

And you know, it kind of placated some of the parents in town. Well, you know, they are sending her for help. You know, let's hope that she is not crazy.

It became so bad, in fact, that I went away to boarding school. I had to leave. I had to get a clean slate.

And we began the judicial process. We learned that we could try Frank under the 1996 Communications Decency Act, but it was the first case and it required a lot of time. While most kids remember their adolescence making themselves up to get ready to go to dances or preparing for dates or going to the movies with friends, I remember cleaning the house getting ready for the FBI to come. I remember taking a polygraph test. I remember testifying for a grand jury.

I do not remember getting ready to go to the dance. It took 2 years to finally prosecute Mark and in that time, he first pled not guilty and then eventually did. The FBI uncovered that he had actually done this to several other girls, some using the Internet. Some he had hired locals in his community that worked with him at his office. And he had even done this to a boy. He had downloaded images regularly of child pornography that they traced through the Images Project.

It was very hard for me to admit that this person that I knew could do this. I still longed for Mark, and I had to admit that this was really Frank. So I felt a lot of guilt. I felt that I was sending my friend to jail. Jail was a spot on the Monopoly board that you could pay fifty bucks to get out of. We could not do that with Frank.

I knew where he was going and I felt very, very guilty. In fact, that guilt consumed me so much that one time I found myself in the shower with all my clothes on. I did not even know how I had gotten there.

I then went to a psychologist and a psychiatrist. I was prescribed Buspar, which is an anti-anxiety prescription, and I was throwing up all the time, almost daily. I had blood vessels popping on my skin. And I was diagnosed with clinical depression.

And I share this not to gross anyone out, but to share that it was a really difficult time in my life and that it does go on for quite some time.

Frank eventually pled guilty and was sentenced to 18 months in jail. He has since been released. And I knew that that really was not the answer when he was sentenced. I did not feel that this was the end of it.

Immediately after his sentencing, I came home and I began writing. I do believe that if it could happen to me, it could happen to any one. And I wanted to share my story with other girls across the country, which is why I wrote Katie.com. Hopefully they can read my story and see, well, if it could happen to Katie, it could happen to anyone.

Everyone wants to know what is different about me. What is so special about me that I could have been a victim of the Internet? Why me?

And they might want to blame the fact that my parents are divorced so that I would be one of those alone and isolated cases. Or they could think, "Well, she was promiscuous. Maybe she was looking for a boyfriend."

I mean, we have to classify victims of sexual assault in some way, it seems, as our society says. But the real fact is that I was 13 and I was vulnerable. And pedophiles know this and they prey upon it.

So I do think that there needs to be some kind of measure or monitoring of the Internet because parents cannot be everywhere. While some computers do have filtering software, that is not on every computer.

As I travel the country, everyone thinks, "Well, this is never going to happen to my kid." and they will tell me how intelligent they are, how special they are.

I could say the same, that I thought I was never going to be a victim. I believe that if there were some type of monitoring system in place and if there was more education back in 1995, I do not think that I would have been a victim.

I do not think that I have anything to add because there are so many experts from this field, and the best thing that I could offer is my own story. So at this point I will close and I thank you.

[The prepared statement of Katherine Tarbox follows:]

PREPARED STATEMENT OF KATHERINE TARBOX

I was thirteen years old when I first started using the Internet. My parents received a disk in the mail offering my family free hours of America Online. This was 1995 and we didn't completely know what the Internet would bring into our home. The news focused on how this would help our lives; we could buy airplane tickets and my sister would be able to do a complete college search. We didn't think there were any potential dangers to having our computer plugged in with millions of others. We were wrong.

I had used America Online once before at school with a project we were working on through CNN and thousands of others schools to help save the Everglades. We used the chat rooms to learn what other schools had done. We only went into chat rooms, and I didn't know that the Internet was meant to be resource tool and a communication tool. From the beginning of my Internet use, I thought of it as a place to meet people. I think I thought of the Internet the way an adult goes to a bar, they go there to meet people.

When I first started using America Online in my house, I only went into teen chat rooms. I found some to be overly sexual, but for the most part I found people who I thought were teenagers. We would talk about our common interests, which could be swimming, popular bands, or movies. I didn't use it excessively, but found myself logging on about an hour a day. This is far less than the average child spends online today.

It was a September Sunday morning when I met a guy in a teen chat room named Mark. I asked if anyone wanted to talk to a thirteen-year-old girl from Connecticut, and he replied. I immediately found out that he was twenty-three years old and from California. I sat there and stared at my computer questioning if it was all right for me to talk to a twenty-three year old man. At first, I said no; however, I then said to myself "this is only on the Internet, it can't hurt." I honestly didn't think I would have much in common with an older man, nor could I understand why he would have interest in talking to me. All this intrigued and persuaded me to continue.

Mark asked what my favorite bands were. I answered, and then he also said he liked them too. Not only did he like those bands, but also he had been to concerts and could name his favorite songs. He then asked me where I shopped. Ironically, he also shopped there. He could also tell me styles that he had purchased there and products he frequently bought. We then talked about places we had both traveled to, and movies we had both seen. While the FBI may call this process grooming, in my thirteen-year old mind this was fate.

At that age I didn't even know what a pedophile was. And though I didn't know what a pedophile was, I instinctively knew that I couldn't be a victim of one. I was a high-honors student, a national swimmer, a very accomplished musician, and I came from a loving family. Our society has labeled victims of sexual assault as being alone and isolated, or promiscuous. I wasn't those things, and so I never thought I could be talking to a pedophile. More importantly, the D.A.R.E. classes that I had in school taught me that rapists are usually uneducated and scary people. Mark was a very intelligent and caring person. This translated for me that Mark couldn't be a pedophile.

We developed a friendship over a period of six months. It was platonic, and I can't emphasize that enough. It wasn't sexual. We would talk about politics, world issues, and a lot of pop culture. I could tell him my concerns about school, friends and family. This led me to believe that my friendship with Mark was beneficial in my life. I believed he was a positive influence in my life. Mark told me the things that I needed to hear at that age. He told me I was intelligent, beautiful and mature. At thirteen, while trying to develop a sense of identity, my confidence level is very low.

There was continuous pressure from Mark to have an in person encounter. I wanted this, but didn't see how logistically it would work out. He was from California and I was from Connecticut. I knew I wouldn't go to California, and I didn't think it would be ok to have him over to my house. I hadn't told my parents about this relationship, because I didn't think they would understand the nature of it. I thought they would dismiss it as something sexual, when it wasn't, and force me to end it.

Mark kept on suggesting times that we could meet, and I told him that I couldn't because I was going to Texas for a national swim meet. Mark said he would come along with, and before I could say no, I said yes. It was one week before the actual visit, and I was always in the honeymoon excitement period of finally meeting him. This excitement prevented me from rationalizing that I was going to meet an older man from the Internet.

I traveled to Texas with my swim team and my mother. I stayed with one of my close friends, and my mother was down the hall. The friend that I was staying with was the only person I had told about my relationship. As I suspected, she passed it off as a sexual relationship. This reaffirmed that I was a little more mature than the rest of my friends, and could handle this friendship with Mark.

At 9:30 Mark called my room and said he wanted to see me. I immediately headed for the door. My friend, Kerry, insisted that I didn't go and held herself against the door. I pushed her to the side, told her the room number of Mark's hotel room and headed to the elevator. I know the scariest part in all of this is that I never thought I was putting myself in a dangerous situation. I never thought I could be raped, or killed. I never thought Mark would be any other person than who he said he was.

I knocked on the door and he opened it. We had exchanged pictures, but his was taken from so far away that I couldn't make out any distinguishing features. Standing at the door, I realized that this was an adult. I knew he was an adult, but on the Internet a lot of fantasy gets built up and you don't have to acknowledge reality.

I felt very uncomfortable to be with Mark. He sensed this and began talking about the airport, soap dishes, my shoes, and other random subjects. He bounced around on topics, hoping to put me at ease. While there, I didn't know what was going to happen and I thought we would continue to have conversations like we had had over the phone.

I had been there about thirty minutes, when Mark leaned over and said, "Katie, I have been thinking about you all day and thinking about doing this." I knew what this was. He leaned in, kissed me, then groped me, and touched other parts of my body. Essentially, in those short fifteen minutes, I was molested.

I always thought that if I were in a position where I was receiving unwanted sexual advances that I would be strong. Instead, in the moment, I became passive. I was confused. I thought, "Do I owe to Mark? Of course he didn't come from California just to talk." I was disappointed in myself and felt very dirty as a result of him touching me.

There was a knock on the door, and my gut could tell it was my mother. I knew how disappointed she was going to be, though I felt relieved that I was going to be saved. I know if she didn't come, I would have been raped that night. My friend had told my mother where I had gone. My mom gathered hotel security and police and came to the door.

The police questioned me and I told them briefly what had happened, carefully leaving out what Mark had done physically. They came back and said, "Miss, we have been talking to him for ten minutes and you say you have been talking to him for six months. His name is not Mark, but it is really Frank Kufrovich. He is not twenty-three, but actually forty-one. He is also a financial advisor from Los Angeles." As they told me this, I thought, "Who the hell had I been talking to?"

I realized that Frank could be doing this to anyone. At the same time, I didn't want to admit that Frank had lied to me. It was very hard for me to admit that Mark was a made up person, and that Frank was sick pedophile. I came forward and my family pressed charges, because I knew deep down it was the right thing to do. It was hard though, and I felt like I was betraying a friend.

It took two years to prosecute him. In that time I lost all my friends at school because parents and my classmates blamed this on me. I eventually had to go away to a boarding school so that I could have a clean slate. Frank hired private inves-

tigators, who came and interviewed people in my town. I suffered from tremendous guilt, and I was diagnosed as being clinically depressed. I was taking a very high dose of Buspar, an anti-anxiety medication, which made me vomit almost daily. I had blood vessels popping on my skin making a rash. I even found myself in a shower with all my clothes on, not knowing how I had gotten there. I remember my adolescence by the times I went to the FBI for a polygraph test, or going to the psychologist. I don't remember putting on make-up preparing for the school dance. I think about that time as living hell.

Frank eventually pleaded guilty. He was charged under the 1996 Communications Decency Act with traveling interstate with the intent to have sex with a minor and using interstate communication to persuade a minor to have sex. Frank was sentenced to a mere eighteen months in Federal prison. He was released in October of 1999, and will be off probation by the end of this summer. The FBI found that Frank had raped several girls, and even a boy. He also married a girl that he began sleeping with when she was just thirteen years old.

I wrote about my experience in my book, Katie.com, because I wanted girls to be empowered. While traveling around the country, speaking about my experience with the Internet, the most common question I get is "What do you think was different about you that would make you a victim?" I am sure they want to blame the fact that my parents were divorced, or use the excuse that my mother is a work-a-holic. These are not the reasons why I became a victim. The answer is that I was thirteen. Thirteen is a very vulnerable age, and it happened that I met someone who told me the things that I needed to hear at that age. This is especially true in today's society, where girls are told to live up to very unrealistic expectations. Every person is thirteen at some point, and every thirteen year old is vulnerable. Though their parents may think they are safe while on the Internet, they are not.

There needs to be some type of regulation to control chat rooms on the Internet. Unfortunately there are too many pedophiles out there, and at the same time, there are many vulnerable teenagers using the Internet. Some of them may not give out their address, or their real name, but they give out other personal information, like their number on the field hockey team and their school. This is enough for a person to find them.

Children don't realize the consequences to Internet relationships. I know this because I have communicated with thousands of girls through my website. If they don't know the consequences they will learn them, unfortunately, probably the same way I did. We need to step up and protect children while they surf the Internet. The Internet is an incredible tool, and should be used by all; however, it should be safe.

Mr. UPTON. Thank you very much, Katie. It is a nightmare that no family wants to experience, and we certainly appreciate you sharing your experiences with us today. Thank you.

Our next witness is John Karraker.

John, welcome.

STATEMENT OF JOHN KARRAKER

Mr. KARRAKER. Thank you.

Chairman Upton and Congressman Bass, thank you for the opportunity to testify today at this hearing entitled "Chatting Online: A Dangerous Proposition for Children." Katie, your compelling story makes me realize how lucky I am and how lucky my family was. I appear today before you as a private citizen representing myself and, more importantly, as a father.

My oldest daughter was nearly a victim of a sexual predator. I allowed her to engage in chat room conversations and utilize the Internet when I was not home.

I found a phone message from somebody who sounded much older than my 13 year old daughter asking her to call him. When I questioned her about it, she denied having any knowledge of who this person was.

Shortly afterwards, my ex-wife took a phone call in which the subject mistook her for my daughter. When he refused to answer her questions, she hung up on him.

My daughter, at this point, still refused to provide details, but did admit to a long period of chatting with this person on the Internet and how he had eventually asked her for her number, which she did provide.

I checked the computer for information, but this was not useful. She had deleted any information on identities from her Instant Messenger after being confronted on the first phone call.

I believe now that she was trying to protect him, and if I had not disabled the Internet when I was not home and taken its use away except for monitored homework, it would have continued.

The experience my daughter had fortunately did not have a tragic outcome, but I have to admit that it was more by luck than by parental intervention. We tried to instill in my daughter the possible dangers of meeting people on the Internet. We tried to tell her about sexual predators who were out there, people who would say anything to her to try to establish trust with her.

Unfortunately, I then relied on the judgment of a young girl to make appropriate decisions. The computer was in its own room and I did not physically oversee its use.

Parents must educate themselves and their children with the dangers of the Internet world. Monitoring must consist of more than just reviewing histories on the Internet. Children quickly learn how to delete histories and they will do it.

Reliance on for-profit ISPs will be useless. When I contacted AOL, their attitude was they could care less. I tried to ask them for assistance and they told me that there nothing they could do.

Law enforcement was also of no use at that time. Neither Federal nor local agencies would intervene as there was no crime committed. Even as a police officer who knew some of the type of individuals that exist in our society, I was lax. I thought that I had done my job by warning her.

I have to admit that I also felt very frustrated that as a police officer, I could not make the system work for me and get somebody to take action.

I would just like to express my opinion on several things that could and should happen. First of all, parents must educate themselves and their children and monitor activity. This is probably the most important piece.

ISPs must be held accountable for what happens on their service.

Laws must be enacted that allow law enforcement agencies to pursue potential predators.

Finally, law enforcement agencies must be provided funding for equipment, training, and manpower. I can tell you as a police officer on the street that we do not have the knowledge that we need to have to take enforcement action or to recognize what the problem is.

This problem is not going to go away, but it is only going to become larger.

Thank you for your opportunity to address you.

[The prepared statement of John Karraker follows:]

PREPARED STATEMENT OF JOHN KARRAKER

Congressman Upton and other Members of the Subcommittee, thank you for the opportunity to testify today at this hearing entitled: *Chatting On-line: A Dangerous Proposition for Children.*

I appear before you as a private citizen representing myself and, more importantly, as a father.

My oldest daughter was nearly the victim of a sexual predator. I allowed her to engage in chat room conversations and utilize the Internet when I was not home. I found a phone message from somebody that sounded much older than my 13 year-old daughter asking her to call him. When I questioned her about it she denied having any knowledge of who the person was. Shortly afterwards my ex-wife took a phone call in which he mistook her for my daughter. When he refused to answer her questions she hung up.

My daughter as this point still refused to provide details but did admit to a long period of chatting with this person on the Internet and how he'd eventually asked for her number, which she provided.

Checking the computer for information was not useful, as she'd deleted any information on identities from her instant messenger after being confronted on the first phone call. I believe now that she was trying to protect him and if I'd not disabled the Internet when I wasn't home and taken it's use away except for monitored homework, it would of continued.

The experience my daughter experienced fortunately did not have a tragic outcome, but that was more by luck than parental intervention.

We tried to instill the possible dangers of meeting people on the Internet with my daughter. We tried to warn her of sexual predators who would say anything to lure her into meeting them. I told her they would try to establish bonds with her to make her trust them. Unfortunately I then relied on the judgment of a young girl to make appropriate decisions. The computer was in it's own room and I did not physically oversee its use.

Parents must educate themselves and than their children with the dangers in the Internet world. Monitoring must consist of more than just reviewing histories of Internet use. Children quickly learn how to delete histories and will do it.

Reliance on for profit ISPs will also be useless. When I contacted AOL their attitude was they could care less.

Law enforcement was also of no use. At that time neither local nor federal agencies would intervene when no crime had yet happened.

Even as a police officer who knew of some of the types of individuals that exist in our society I was lax. I thought I'd done my job in warning her. I also felt very frustrated that even as a police officer, I could not get anybody to take action.

In my opinion several things must happen:

- Parents must educate themselves and their children and monitor activity.
- ISPs must be held accountable for what happens on their service.
- Laws must be enacted that allows law enforcement agencies to pursue potential predators.
- Law enforcement agencies must be provided funding for equipment, training and manpower. This problem is not going to go away but only become larger.

Mr. UPTON. Thank you very much, John.

Our next witness is a prosecutor in Kalamazoo County, Jim Gregart.

STATEMENT OF JIM GREGART

Mr. GREGART. Mr. Chairman, Congressman Bass, my name is Jim Gregart. Believe it or not, I am the "Ponytail Prosecutor" for Kalamazoo County.

I have been in criminal justice for over 40 years. At the beginning of my career, I would have thought this day of me testifying about computers and something called the Internet would have been as much lunacy as thinking of putting a man on the moon, but my, don't things move quickly?

When first asked if I had anything to add to this hearing, I told Congressman Upton and staff, "Well, sure. We have cases in Kala-

mazoo. There are not as many as large metropolitan areas, but we have some."

And then I asked my staff to bring together all the closed and open files and found out that we had more than I had thought. In a variety of different ways, the computer and technology have become part of America's criminal justice system.

So in order to get an average fact pattern, I went through the cases we had. And then last Thursday at exactly 4:45 p.m., one more walked into my office. One of my team leaders said, "I understand you are going to testify next week." And then he handed me the charges he had just authorized against Kalamazoo's latest cyber predator.

This kind of crime emanating, having its origins in chat rooms is not a widely reported phenomena, and yet it is occurring much more than we would like to admit, I believe, in America, somewhat like the status of domestic violence many years ago. There was a proliferation of it, but our polite society kept it below the genteel surface of public acknowledgement.

Today there are many, many, many, many children being subjected to sexual assaults emanating originally from a contact made in an Internet chat room. Most of those instances are not being reported to the authorities for a variety of reasons, many of those articulated well by Katie.

By the way, not only are you a survivor. You are a winner. You do not have to worry about your future. You are going to do exceptionally well.

But here is the latest one from Kalamazoo. A 34 year old Kalamazoo County resident posing in an Internet chat room as a 17 year old high school student begins a relationship with a 14 year old high school freshman from another county in Western Michigan. Over a period of time, it results in a meeting, a personal meeting, and ultimately a sexual relationship of a 34 year old adult male with a 14 year old female.

That particular defendant now faces up to 35 years in a Michigan prison upon conviction. And we intend to convict the defendant.

I grew up with the parental admonition of "do not talk to strangers." Most of us did. Do not talk to strangers, and yet everyday in this Nation, in this state, and in this Middle American, quasi-agrarian community of Southwest Michigan, we have parents who repeatedly let their children talk to strangers.

As John indicated, and I reinforce and validate, parents have to learn technology. I am a dinosaur. I am not hard-wired like young people today. I tried to stave off the tsunami of computer technology beyond my professional career. And then 1 day I was just swamped. Technology came over the gunnels of my personal ship. So I had to learn technology.

I have and I am now an information junkie on the Internet. Wow, it is a sad day when somebody like me starts learning about technology.

Nevertheless, a lot of parents today intentionally remain removed. They will buy a computer. They will sign up for Internet service, and they will trust that their children will only use it for

legitimate, educational purposes. Perhaps they, too, as I once thought, think that they are too old to learn about technology.

Well, not taking the time to learn about technology is to do the equivalent of putting their children untrained, immature, behind the wheel of an automobile because that is the potential harm that can result. Nobody today in their right mind would think about letting their child without any kind of training, without any kind of experience, without any kind of guidelines, at the age of 12 or 13 get behind the wheel of a car and just take off wherever.

Well, that is what happens when you get on the Internet. It is a cyber-playground; you can go anywhere in the world. You are a mouse-click from Europe. You are a key stroke from the Pacific Rim countries or you are a nanosecond from an adult pedophile predator.

And they are lurking out there, believe me. Who would think that this is not Silicon Valley? This is not a big major metropolitan are. This is Kalamazoo; this is Southwest Michigan.

But they are here. They are here, and they are not all down the street opening a car door and saying, "Hey, little girl, want to see a puppy?" or "hey, want some candy?" That is old kind of traditional view of someone who is trying to snare a child into his lair.

Instead, they are not in cars on our streets. They are not walking around our playgrounds. Instead, they are in your own child's bedroom, if that is where you happen to keep a personal computer, or they are in your family room or they are in your den because they come to you almost close enough to touch your child via the Internet.

I remember how proud I was in the early 1990's taking my two children to a seminar about the Internet because in the early 1990's it was truly an emerging technology. After we got our PC and we signed up with AOL, I remember them sitting at the table and saying, "Guess who I talked to last night? Somebody in South Africa, somebody in Japan, somebody in countries all over the world."

I thought, "This is terrific. What a cultural opportunity and education."

And like a dolt, John, you and I share. I guess this is True Confessions time. I never thought in the early 1990's about what could happen.

There are hundreds and thousands of parents today, who have not yet realized the potential risk that their children are at. Katie's folks know; John knows; I know. Hopefully the majority of people in this room know. But yet there are hundreds and thousands of parents who still today let their kids get behind the wheel of a Ferrari at the age of 13 or let them talk to the stranger who opens the Internet door in the chat room and become inveigled.

Kids at 13 and 14 are vulnerable. Let's admit it. Katie, you well articulated the vulnerabilities of an average youngster in America today.

Are there lessons to be learned? Yep, from the old, grained prosecutor in Kalamazoo.

No. 1, parents/custodians have to learn at least a modicum about technology, computers, and the Internet. You cannot blindly and

blithely raise children without having some awareness of the benefits and the harms that are out there.

Children, themselves, ought to be given some sort of training as to the appropriate use of the Internet and chat rooms.

Third, a matter of sensitivity, and that is called monitoring. There are a variety of ways to monitor a child's use of chat rooms. Some of them are rather explicit and express. And then there are others that are more shall we say I will choose the word "secretive," clandestine?

In one recent case in Kalamazoo County, I have here the instant messaging printouts that a parent took off of his child's computer. This relates to a charge of sexual assault against an adult male preying upon a young juvenile.

But there are software programs available where parents can not just monitor keyboard strokes and track that, but even instant messaging now.

So if I can say one thing to parents, "do not let your children talk to strangers, not just in the playground or out on the street, but in your own home."

Thank you.

[The prepared statement of Jim Gregart follows:]

PREPARED STATEMENT OF JIM GREGART, KALAMAZOO COUNTY PROSECUTING ATTORNEY

I'm Jim Gregart, the elected Kalamazoo County Prosecuting Attorney. Don't let my ponytail fool you. I'm a law & order former police officer from Detroit and have been a prosecutor in Kalamazoo for the past 32 years. I first began my career in criminal justice just two years after the Detroit Lions last won an NFL championship. That fact alone gives you some idea of my professional longevity and the vast changes I've experienced in the nature of crime in America.

As a criminal justice college student in the 1950's, the idea of me someday testifying before a Congressional Subcommittee on something called "Internet Computer Crime" would have been equally screwy as putting a man on the moon. Nevertheless, today my job requires that I both regularly use and understand a complicated technology that was only "science fiction" a mere 15 years ago.

When Congressman Upton asked me to testify at today's hearing, I had my staff pull our closed and pending files on computer crimes. To be honest, there weren't that many. You see,. . . the Prosecutor or District Attorney usually sees a criminal case only when the police first have a crime reported to them and then only when they're able to uncover sufficient admissible evidence to support a provable offense. The lack of victim reporting is the first impediment to the successful prosecution of adults who use Internet chat-rooms to prey upon children.

All reasonable people acknowledge that this type of crime occurs in America. But, the reporting of it to law enforcement officials can be likened to an iceberg, i.e. we only see a small portion of a much larger mass which lurks beneath the genteel surface of millions of legitimate Internet communications. Untold numbers of chat-room initiated sexual assaults of children are not reported to the police because either (1) the actual child victim chooses not to disclose the offense, or (2) parents or guardians are unaware that the offense occurred, or (3) the Constitutional right of a criminal defendant to confront and cross-examine their accuser in a public trial sometimes acts as a subtle deterrent to reporting the crime.

It takes genuine courage for a victim and their family to do what's right; even though it may be difficult and personally embarrassing. I'm aware of cases in my jurisdiction where victims and their families have chosen not to cooperate with law enforcement investigators. Thus, their alleged assailants have never been brought to justice.

However, that was not the decision made by one West Michigan child and her family only last week. This 14 year old high school student and her family are cooperating with local law enforcement officials. Because of their cooperation, this child's 34 year old Kalamazoo sexual assailant now stands charged with a violation of Michigan's law prohibiting the Use of Internet Communications to Commit a

Crime and two (2) additional Counts of Criminal Sexual Assault. Upon conviction, this pedophilic cyber-predator will face up to 35 years in a Michigan prison.

To some folks, Southwest Michigan may seem far removed from the threat posed to children by adult Internet chat room predators. However, nothing could be further from the reality of today's technologically shrinking world. Anyone sitting at a computer in Kalamazoo is merely a mouse-click away from anywhere in the world. Any child could be merely a keystroke and nanosecond removed from the chat room babble of a masquerading adult bent on predatory sexual assault. In my community, we've had adults travel from other states to sexually assault local children whom they've first encountered and deceptively cajoled via Internet chat rooms.

Last week's case, however, is uniquely Michigan. The defendant lives in Kalamazoo county while the 14 year old victim resides in another West Michigan community. Late last year, the chat-room phenomena brought them together in cyberspace. This 34 year old adult identified himself to the victim as a 17 year old high school senior. The victim, however, readily identified herself to the defendant as only being a 14 year old high school freshman. Over a period of time, their keyboard communications transmuted into a personal meeting and, ultimately, repeated acts of sexual assault. Fortunately, this young girl has the personal courage and strong support of her family. They evidence a determination to pursue justice.

Since this criminal prosecution is currently pending in our local courts, I'm not at liberty to publically provide details of the offense. That would be prejudicial to the defendant's Constitutional right to a fair trial. However, I can tell you that, with a court ordered Search Warrant, we've seized the defendant's computer and allied records. The police now have a list of approximately 20 additional female names that they've starting checking. Right now, we have no idea of the ages of these females. But, we will soon find out.

Are there lessons to be learned from this most recent and other similar cases in "middle America"? Yes,. . . and, the first one is to recognize and acknowledge that crimes like this can and are happening everywhere in this Nation; even in a quasi-agrarian area like Southwest Michigan.

Secondly, parents and guardians can no longer blithely ignore the tidal wave of technology which has engulfed our society. Not too long ago, I honestly thought I could stave-off learning about computers until my life expectancy and net worth simultaneously arrived at "zero". Boy, was I ever wrong! And today, any person responsible for the well-being of a child would also be wrong to not educate themselves about both the promise and perils of computers and the Internet.

When the automobile was first invented, it changed the world much for the better. However, when driven recklessly by young people, that same automobile can become an instrument of peril and death. Most adults would not place their child behind the wheel of this potentially dangerous machine without first providing adequate education, training and constant monitoring of their child's driving performance. Well, computers and the Internet hold the same promise for both positive and negative outcomes for children.

When used properly, the Internet and chat rooms can be a wonderful experience for children. But, without adequate preliminary education, safeguards and monitoring, they can become the equivalent of putting an untrained youngster behind the wheel of a Ferrari and hoping for the best. In today's world, the technological speed of a computer chip almost seems to be rivaling that of a Ferrari. The reckless use of a motor vehicle can hurt a child. That same reckless and uncontrolled use of the Internet and chat rooms can likewise place children at risk of physical and emotional harm.

When I was a child, I remember my parents repeatedly telling me, "Don't talk to strangers". That was good advice back then and I gave my own children that same constant admonishment. My kids are now in their mid-twenties. But, as I look back to their teen-age years, I'm chagrined to admit that I knowingly permitted them to violate my own warnings. As a matter of fact, back then, I was ignorantly pleased when they told me about their new young cyber-friends in far away countries who they met via Internet chat rooms. Fortunately for everyone, my children benefitted immensely from their early exposure to foreign kids and cultures. For them, it was a meaningful educational experience. However, ten years ago, it was also a risk of harm that I didn't fully comprehend or appreciate.

Today in America, parents continue to warn their children about the dangers of "talking to strangers". What many parents don't yet fully understand is that those same "strangers" are not just on public streets or parks. Today, the "strangers" to be feared may also lurk in your own family room or child's bedroom. They live behind the innocent facade of a computer screen and talk to your children in chat rooms on the Internet. In an earlier time, they were the same "strangers" who par-

ents feared would lure their child into their grasp with promises of candy or a puppy.

Now, those very same "strangers" use the anonymous cover of an alias Internet identity to disguise themselves as children. They now use a keyboard to probe for the emotional vulnerabilities of unsuspecting youth. They're the same predators of yesteryear who now use Internet chat rooms in lieu of an open car door and an offer of candy or a lost puppy. The challenge for today's parents is to insure that children "don't talk to strangers" both outside and inside their own homes via unfettered, unmonitored Internet and chat room access. Thank you.

Mr. UPTON. Thank you very much, Jim.

Ruben Rodriguez, thank you so much for coming out from Washington today.

STATEMENT OF RUBEN D. RODRIGUEZ

Mr. RODRIGUEZ. It was my pleasure, Mr. Chairman, Mr. Bass.

I have written out a bunch of the things that I wanted to talk about. But listening to Katie's story, I have had the pleasure of appearing with Katie before, and I echo the earlier comments that she is a very brave young lady and we hope to work with her in the future, absolutely.

Let me tell you a little bit about the National Center. The National Center has been in creation since 1984. While everybody knew for many, many years that the center was the clearinghouse for missing children, nobody really knew about the other resources and the other issues that we have dealt with, and that obviously was the issue of the exploitation of children.

Before coming to the National Center 12 years ago, I spent 20 years in law enforcement in Washington, DC, working with traditional crimes. And only when I started at the National Center did I really ever work on children-related issues, more so in 1997 when I took over the unit, and I started seeing the problems that are out there on the Internet.

When I was in law enforcement back in the 1970's and 1980's—I am dating myself now—there was no such thing as the Internet and computers. We were still using typewriters and word processors for computers, and most people did not even know to spell the Internet, other than use it, and that was in law enforcement.

And I thought that we were cutting-edge in Washington. Since I was able to work on data bases, it was very helpful. But then the Internet was another world that we knew nothing about.

When I started at the Center, still the Internet was not an issue. The National Center's Web site did not go into production until 1995 anyway or 1996. In 1997 we developed the Exploited Child Unit. And in 1998 we developed the Cyber Tipline to allow the public to report incidents of child sexual exploitation.

In the first year of operations, we had over 17,000 reports. Today we have over 71,000 reports; 1600 of those have to do with chat.

Now, it does not seem like a large number when you say 1600 compared to 71,000, but when you look at the history of these individuals in these cases, most of these cases go unreported because parents, like John said, become aware of it and they say, "Well, we have stopped it. So we can take care of it. It is not a problem. We have already reported it to the on-line service provider. We have, you know, put in software to stop access to the Internet and block access to the Internet. The problem is solved."

Of course, not knowing the predator or the sexual molester or cyber pedophile, whatever you want to call it, these individuals do not do this once. They have been out there for years. They have been sitting there doing this via mail, on the playgrounds, and now they have this medium, this anonymous medium, to communicate among themselves and also go into predicated areas to find children.

I use the analogy of if you want to go to buy meat, you go to a meat market. When you want to go find children on the Internet, you go to areas where children congregate.

These individuals are experts in the seduction of children. They spend hours and days sitting on the computer. Katie mentioned that this individual knew everything about music groups, songs, name albums. And this is what they do for a living.

If I am looking for a 15 year old child on the Internet, I am going to learn what are the interests of these individuals. What is the interest? How can I get to them? How can I get close to them?

They will spend days and hours. What most people do not realize about chat is that it is a one dominion environment. You can have simultaneous conversations with dozens of people at the same time, different levels of seduction. They do not mind spending months, weeks, and years going after kids because there are so many of them out there that they do not mind investing the time and the effort. All they have to do is hit one and they have dealt with their fantasies. They have taken it beyond that.

Mechanism of chat is made to order for these individuals. Direct text communications: you have a captive audience. A child is looking at a computer screen and so you have their full-time attention. And you can manipulate, build trust relationships, as Katie mentioned. They want to be your friends because the ultimate conclusion for them is sexual motivation. They want to go meet this child.

Most individuals enjoy just the fantasy of it. Unfortunately, there is an all-too-large group that want to go beyond that and actually meet the children.

The numbers are growing. Federal law enforcement officers, State and local law enforcement agencies are getting funding to do these programs. It is not enough. Not so much for the Federal entities, but the State and local law enforcement officers, as he mentioned earlier.

Your victim is local. Your law enforcement agencies are local. You have over 17,000 law enforcement agencies in the United States. You have three major law enforcement agencies: the FBI, U.S. Customs, and the U.S. Postal Inspection that work child pornography related issues, traveler cases, whatever.

But it is your State and local law enforcement agencies that have the areas where the suspect lives and where the child resides. So I would obviously encourage the use of Federal funding to go into those initiatives.

I am privileged to belong to the Internet Crimes Against Children Task Force's Board of Directors. Thirty regional sites throughout the United States are working this issue. Michigan has an I-Tec task force that is very proactive.

I would like to see many of those throughout the United States to help State and local law enforcement agencies, to train them. It

is not really investigation they are involved in. They are also involved in outreach to the community.

There are several programs that work effectively throughout the United States. And I would like to see more funding going into those initiatives.

I can sit here and spit out numbers, and it does make some sense when you are looking at the totality of the problem. But we are just touching the tip of the iceberg. The problem is much bigger than most of us realize.

There was a study done by the FBI in North Carolina at a rehabilitation hospital, where they talked to offenders who had molested children. And the first time they talked to the offenders, they admitted to doing 4 or 5 children. They were talking to, I think, 30 offenders.

When the study was over, they averaged that each one of these offenders were doing at least 300 children before they were apprehended. So the problem is getting bigger.

As the Internet fueled this, it has allowed access. These individuals used to go to the playgrounds, used to look at children, follow them, stalk them. Now they have a medium where they can do it without any risk to themselves.

The risk is when they actually go to meet the child. In many cases, as I mentioned earlier, fantasy is sufficient for them. Unfortunately, there are those who take the fantasy beyond that. They use child pornography to lower inhibitions of the child. It is not so bad. The child is smiling. Different levels of undress. All of that is used by chat. You can append images and add information, URL information.

It is a community where kids are curious. They go out there and put themselves in harm's way unfortunately, and because of their curiosity, they are very trusting, as Katie mentioned. They are somewhat flattered when an individual pays attention to them, when they tell them, "Yeah, I am just a little bit older than you. I am 18, 19, 23," when unfortunately the gentleman is 45 or 50 years old.

We see it all too often. At the National Center we see this information coming on in avalanches now. I say the first time that we started this, we had 17,000 reports. In less than 4 years, we have 71,000, and we are just touching the tip of the iceberg.

The ISPs have come to the table because they were forwarding information to us on not only child pornography, but also on unsolicited E-mails and chat complaints which is great for us. Of course, it is making my work load much higher and hard, but, again, that is our job.

I could go on and on, but I just wanted to agree with many of the things that were said here before me: effective prosecution, funding for law enforcement, and outreach programs for children and parents.

The first line of defense is the home. The analogy again is when you want to teach a child how to drive, you do not throw them a set of keys and say, "Have at it." You sit with them, teach them the rules of the road. You praise them when they do well and correct them when do wrong.

People do not think of the Internet and the computer as the same. It is. You turn on the computer and you let the world into your home.

Thank you.

[The prepared statement of Ruben D. Rodriguez follows:]

PREPARED STATEMENT OF RUBEN D. RODRIGUEZ JR., DIRECTOR, EXPLOITED CHILD UNIT, NATIONAL CENTER FOR MISSING AND EXPLOITED CHILDREN

SUMMARY

Mr. Chairman and members of the Committee, I am pleased to appear before this subcommittee today to express my views on the potential dangers of unsupervised online chatting by our nation's youth. As a way of introduction, I have been involved with the National Center for Missing and Exploited Children and the issue of missing and exploited children since my retirement from the Metropolitan Police Department of Washington, D.C. in 1990. In 1997 I was made the Director of the Exploited Child Unit. One of the mandates of this unit was the creation and development of an online reporting mechanism for the public to report incidents of child sexual exploitation. To date we have received over 71,000 reports, 1,600 of those reports are attributed to the use of chat to entice, seduce and exploit children.

While this medium has offered great opportunities for children and adults alike to conduct research, communicate, meet and chat with new friends throughout the world, unfortunately in certain instances it has also become a vehicle for those who prey on the unsuspecting. Oftentimes, criminals misuse new technology before law enforcement acquires the tools and expertise to counter such uses.

The 2000 Census reports that 9 out of 10 school age children, ages 6-17 years of age have access to a computer. In addition, 4 in 5 households with access to the Internet had one or more members using the Internet (44 million households). Recent figures put the current number of children online to an estimated 10.5 million. The usage time by teens between 16-17 years old illustrates that 32% of these youth spend 5 or more hours online per week.

We at the National Center's Exploited Child Unit are aware of serious incidents where children who communicate in web-based Chat Rooms, IRC or Instant Messaging with individuals who they believe are peers or friends, who eventually turn out to be individuals who are not who they say they are. All too frequently, we see children traveling or meeting these individuals and find out all too late that they have put themselves in harm's way.

I have been asked on numerous occasions by the media and parents, "what can one do to safeguard our children?" and I have always believed that it starts in the home. Law enforcement and organizations like the National Center's CyberTipline only get involved when it is too late. We believe that a comprehensive education program should be instituted in the home to address these issues. In this respect the National Center has created NetSmartz, which is the Center's proactive, educational approach to fighting online predators. The materials developed by the NetSmartz Workshop are designed to be a proactive, educational approach to helping children build self-confidence in order to better handle and protect themselves in all types of situations.

THE DANGERS TO CHILDREN ONLINE

Many parents have a false sense of security regarding the risks to their children in cyberspace. They feel that their children are at home, often in their own rooms, doing something positive and useful for their future. Many parents have little knowledge about computers and what their children are doing online, and feel that there is little risk. Similarly, many children view cyberspace as a variation on their computer or video games. As a result, they may not view encounters with people online with the sense of caution or skepticism that they apply to meeting strangers in the "real" world. Further, chat is one of the most popular pastimes of children online. Numbers are hard to come by, however on American Online, over 100,000 people chat simultaneously in over 20,000 chat rooms.[1] Teenagers, especially, enjoy the anonymity and experimentation chat rooms provide. This, combined with a lack of guidance by parents and the grooming and seduction by a sexual predator, may lead to a child's victimization online.

Just as teenagers enjoy the anonymity offered to them through chat, pedophiles also use this avenue to their advantage. Pedophiles organizations were one of the first criminal groups to exploit Internet technology. The computer has provided

pedophiles with "an ideal means of filling [their] needs for validation, organization, and pornography [as well as] finding potential new victims."[2 3]

Types of Risks to Children in IRC

Online Enticement of Children for Sexual Acts: By the year 2002, more than 45 million children will be online.[3] For sexual predators, this makes the Internet the largest existing playground and the fastest way to meet potential victims. Beginning with the "harmless exchange" of personal information, sexual predators empathize with the child's frustrations with puberty and parents and engage him or her in sexually explicit conversations. The predator may send adult and child pornography to lower the child's inhibitions and eventually arrange a face-to-face meeting for sexual purposes. Therefore, chat rooms often become distorted playgrounds for these predators. They can pose as someone else, approach children with seductive offers, and eventually violate a child's privacy and security. As of May 1999, the National Center for Missing and Exploited Children (NCMEC) has been involved in approximately 599 "traveler" cases in which a child left home or was targeted by an adult to leave home via the Internet. As of May 2002 the National Center received of over 1,600 cases involving Chat and Chat Rooms.

Distribution of Child Pornography and Pedophile Materials: The number of pedophiles and child molesters using the Internet is unknown, but the IRC, in particular, is an ideal medium for numerous pedophile activities:

Distribution of Child Pornography: According to some police estimates, as many as 80,000 child pornography files are traded online every week.[4] Pedowatch also reports that approximately 1,500 people join the preteen erotica trading channels on IRC's Undernet everyday.[5] The IRC provides a fast, easy, effective and discrete method to trade images of child pornography.

Exchange of Pedophile Materials: The IRC provides pedophiles the opportunity to engage in discussions regarding their sexual deviance and exchange pedophile information in a relatively anonymous forum. This only serves to assist them to validate and rationalize their behavior. Also, it has been hypothesized (although not scientifically proven) that the easy access to child pornography images and increased ability to locate those individuals who have similar interests in children may contribute to an individual with latent tendencies to act out and sexually victimize a child.

How does the IRC facilitate the victimization of children?

Lack of monitoring: Operators of IRC servers do not maintain any type of logs of what occurs on the channels of their servers. Unless turned on by users through their client software, whatever is said in a channel is lost after an individual logs off of the server.

Channels can be easily created: Channels can be instantly created and can be invite only requiring a password to enter. Since there is no governing body of the IRC, it is easy to establish private chat channels for the exchange of images, pedophile materials and private one-on-one conversations.

Nicknames can be easily changed: Once in IRC, it is extremely easy to create a channel. Unlike chat rooms through online service providers (which have unique and traceable screen names assigned to them), an IRC user can instantaneously change their nickname and re-enter the chat room as someone else. This makes identifying and tracking IRC users more difficult.

Jurisdictional Questions: The IRC is a global medium with no governing body. This, coupled with the ability for a user to download free client software, makes it extremely difficult to regulate. However, individuals within a channel can be held accountable for criminal actions.

Direct Client-to-Client Connection: One of the most useful features of IRC for pedophiles is the ability to send and receive files outside the IRC network. This feature, called Direct Client to Client (DCC), is the most secure form of communication available on IRC. Messages and files sent via DCC are sent by a direct connection (not part of the IRC network) between two individuals; therefore, they are difficult to track unless you are one of the recipients of the message or file.

Law Enforcement Response to Date

The IRC presents unique challenges to law enforcement to protect children from sexual predators. Although it is possible to trace the identities of those using IRC for illegal purposes, evaporation of electronic audit trails, the use of encryption and steganography, and the ease with which predators can avoid detection through fake cyber identities and other computer tricks are challenges law enforcement face every day. In addition, most law enforcement is ill prepared to address computer-related crimes due to lack of training and necessary equipment (e.g., an Internet connec-

tion). In most countries, law enforcement is playing catch up to an exploding epidemic of computer crime.

Recognizing the need for resources to combat Internet crimes against children, the United States government has taken an active role in assisting federal and local law enforcement. In 1995, the Federal Bureau of Investigations (FBI) created the Innocent Images Task Force to conduct and coordinate online undercover investigations on cases in which individuals use computers to lure children into illicit sexual relationships, and to investigate those individuals who produce, manufacture and distribute child pornography. Through March 31, 2002 Innocent Images has opened 7,067 cases, has filed 1,811 Information/Indictments, and has 1,850 convictions. The United States Customs Service also plays a crucial role in investigating child pornography trafficking and pedophile organization cases. They were the first federal law enforcement agency to initiate a comprehensive computer child pornography case. During fiscal years of 1998 through 2001, the United States Customs Service investigations produced 874 convictions.

In 1998, the United States Congress provided the Department of Justice's Office of Juvenile Justice and Delinquency Prevention over two million dollars to create ten Internet Crimes Against Children Task Forces on the local or state level. The ICAC Task Force Program "encourages communities to develop regional multi-disciplinary, multi-jurisdictional task forces to prevent, interdict, and investigate sexual exploitation offenses against children by offenders using online technology."[6] The ICAC Task Force Project has a current financial commitment of over $7,000,000. The Project currently includes 30 Regional Task Forces and over 45 satellite programs, throughout the United States.

What Can Hotlines Do?

Hotlines can play a vital role in protecting children in cyberspace through a strategy of prevention/awareness resources, training and technical assistance to law enforcement and working closely with the online industry.

To provide a reporting mechanism for the public to report incidents of child sexual exploitation: On March 9, 1998, key public and private sector leaders joined with NCMEC to launch the new CyberTipline, www.cybertipline.com. The Tipline was created for parents to report incidents of suspicious or illegal Internet activity, including the distribution of child pornography online or situations involving the online enticement of children for sexual exploitation. Seven days per week, 24 hours per day, NCMEC is fully staffed to handle leads, and then distribute those leads to the appropriate law enforcement agencies.

Effective that day, the FBI's Innocent Images Task Force, the Crimes Against Children Unit at FBI Headquarters, the US Customs Service CyberSmuggling Unit, and the US Postal Inspection Service have immediate access to all data received on the CyberTipline via the web. Thus, these primary federal law enforcement agencies are immediately able to receive, access and review all CyberTipline leads.

The CyberTipline is also uniquely positioned to gather important data on these types of Internet crimes against children. It is the hope of NCMEC to be able to conduct in-depth analysis of trends and patterns in these types of cases in the near future.

To prevent child victimization in cyberspace through aggressive prevention/education and outreach programs directed toward parents and children: NCMEC is seeking to reach into millions of homes and classrooms with positive, common sense rules for Internet safety. Through two publications, *Child Safety on the Information Highway and Teen Safety on the Information Highway,* NCMEC's message for parents focuses upon strong parental involvement in their children's lives, increasing parental knowledge and awareness about computers and the Internet, and the importance of parent-child communication.

Likewise, NCMEC is reaching out to children with basic rules for safety on the information highway, including cautions not to give out personal information online, and not to meet someone they encounter online. A cornerstone of this effort is the National Center's "NetSmartz" initiative. The program goals are to: enhance a child's ability to avoid victimization, reduce the feelings of guilt and blame that are often associated with victimization, encourage children to report victimization to a trusted adult, support and enhance community education efforts and to increase communications between adults and children about online safety.

To advocate help for parents through the development of technology tools and access controls: NCMEC supports efforts to provide help for parents through blocking software and access control tools like SurfWatch, Net Nanny, and similar products, enabling parents to limit areas of the Internet to which their children have access. While such tools should not be viewed as substitutes for basic parenting, nor do they prevent adult predators from going to where the children are

on the Internet to seek their victims, nonetheless they are useful tools for parents to provide an extra layer of protection for their children.

To target and educate those who are most at risk: Parents and teachers are often surprised to learn that young children are not the most common victims of abduction and sexual assault. In fact, twelve to seventeen year old teenagers (especially girls) are the most victimized segment of the United States population.[7] A review of NCMEC data also shows that in 72% of the missing child cases involving the Internet, the victim was 15 years of age or older. In 83% of these cases, the victim has been female. As a result, the *Know the Rules Campaign* was launched in March 1998 as a national public service campaign targeted to girls ages 11-17. The educational messages in this campaign convey strength and are designed to leave girls with a sense of empowerment.

To promote a national campaign of aggressive enforcement: NCMEC feels that the most important element of its Cyberspace Strategy is aggressive enforcement by federal, state and local law enforcement, directed against those who misuse the Internet for criminal purposes. Oftentimes, criminals misuse new technology before law enforcement acquires the tools and expertise to counter such uses. To assist law enforcement, NCMEC is involved in the two courses specifically targeting Internet crimes against children.

- Protecting Children Online Investigator's Course: This 4½ day course is held monthly across the United States, and was designed to enhance law enforcement's ability to investigate Internet crimes against children. Topics covered include: recognizing and identifying computer crimes against children, orientation to computer technology, conducting the investigation, legal issues, case preparation and follow-up, and resources and prevention.
- Protecting Children Online Unit Commander's Course: This 2½ day course is held monthly at NCMEC headquarters in Arlington, VA. The purpose of this training program is to provide law enforcement unit commanders with an understanding of the key management issues for the effective investigation, prosecution, intervention, and prevention of computer crimes against children.

To establish relationships and work closely with the online industry: One of the exciting elements of this initiative is that the online industry is a strong partner. Leading companies including America Online, Microsoft, CompuServe, AT&T, NetCom, the Interactive Services Association, and others are providing financial support and have committed to promote the CyberTipline through their subscribers and supporters.

The following are examples of some of the public/private initiatives involving NCMEC:

- On February 10, 1998 NCMEC joined with SurfWatch, maker of the first Internet filtering product, in a partnership to provide leads to NCMEC and its CyberTipline. SurfWatch is creating an online capability on its website for its users and customers to report child pornography or child exploitation directly to NCMEC and its CyberTipline. We are hopeful that other companies will follow this example, helping NCMEC promote the CyberTipline and provide the most direct linkage for users, so that when they encounter inappropriate or questionable material, they can easily and immediately link with NCMEC's CyberTipline and provide their information.
- America Online began a program with NCMEC called "Kid Patrol," through which NCMEC can take images and breaking information directly to AOL users. It is our vision that this effort will become a kind of two-way communication vehicle using cyberspace.
- Similarly, Lycos, the search engine, has joined with NCMEC to leverage the Internet for child safety, taking images and information to Lycos' users, and making it easier for users to get to NCMEC.

Thank you for the opportunity to express on concerns. As always, I hope you will view NCMEC as a resource. We stand ready to assist in any possible way.

Endnotes

[1] L. Gibbons Paul, Family PC, February 16, 1999, www.zdnet.com
[2] K. Lanning, Use of Computers in the Sexual Exploitation of Children, 1999.
[3] BIND/VP's Emerging Technologies Research Group and Grunwald Associates
[4] ZDNet, 11/19/97
[5] Pedowatch, Pedophilia on the Internet, pedowatch.org
[6] Federal Register: May 7, 1999 (Volume 64, Number 88), Page 24855-24860
[7] Bureau of Justice Statistics Sourcebook of Criminal Justice Statistics—1996. Washington, D.C.: Office of Justice Programs, U. S. Department of Justice, pages 210-11.

WHAT IS CHAT?

Chat refers to an Internet application that allows two or more people to carry on a text "conversation."

Chat is available through: Commercial Internet service; IRC (Internet Relay Chat); and Web-based Chat Service, i.e. Yahoo Chat, etc.

Internet Relay Chat: Internet "chat" function that enables two or more people to carry on a text "conversation." IRC networks are comprised of servers around the world linked to each other. User needs IRC software on their computer to use IRC. User selects a network, server and channel. A "real-time" chat screen opens, allowing typed conversation between people on the same channel.

Instant Messaging or IM: Software is installed on you computer. When you run the software and connect to the Internet you are "logged on" to the service. This gives the service the ability to notify others you are online. You are given the ability to see when selected people are online. You can then exchange real-time, or "instant" messages.

Instant Messaging Software and Users: ICQ—73 Million Users; AOL—65.5 Million Users; MSN—2.8 Million Users; Tribal Voice Pow Wow—10 Million Users; Yahoo Messenger—Undisclosed; Prodigy Instant Messaging—Undisclosed *(PC Week 10/11/99)*

Mr. UPTON. Thank you, Ruben.

Ms. Curtin has also come out from Washington today.

Thank you.

STATEMENT OF CAROLINE CURTIN

Ms. CURTIN. Thank you, Chairman Upton and Congressman Bass, for having me here today to testify on issues relating to child safety in the on-line environment.

I just wanted to take a minute to thank Katie, in particular, for sharing your experience and your courage and your hope. It gives me a renewed vigor and effort in going back to AOL. I will certainly share your story with my colleagues, the people that work on these issues day in and day out.

We know how important they are, but hearing your story renews that and reemphasizes it. So thank you.

As Director of Children's Policy for AOL, I am responsible for coordinating child safety and privacy protections across the AOL properties, as well as educating parents about on-line safety and the importance of parental involvement.

I am pleased to have the opportunity to describe AOL's efforts to educate our members about on-line safety, the tools and resources that we provide for our members, such as our easy-to-use parental controls, as well as our ongoing partnership with law enforcement and other stakeholders to help keep the on-line environment safe for children.

AOL has played a significant role in the development of the on-line media, and we have always shared a special appreciation of its enormous potential to benefit society, especially children.

Learning how to explore and understand the on-line world is an essential skill for our children in today's wired world, but we all agree that kids need and deserve special protection in this new medium. AOL recognizes that parents must have the ability to ensure to that their children can enjoy a rewarding and safe interactive experience on line. It has, therefore, been our challenge to craft rules of the road for children's on-line safety, enabling parents to protect their children while at the same time helping them to take advantage of the wonders of the on-line environment.

By promoting major public education campaigns and closely cooperating with elected officials and government agencies on outreach and enforcement efforts, we have tried to offer strong, proactive leadership in every area of children's safety on line.

Clearly no wall, no technology, no corporate initiative can ever take the place of an educated and involved parent. We have heard that from earlier testimony and I cannot emphasize it enough. This is why we have dedicated significant energy to providing AOL parents with the most useful information, content tools, and safety tips to help protect their kids, as well as a list of resources available for both families on AOL and the rest of the Internet.

By doing so, we have tried to empower parents so they can ensure that their children's on-line experiences are the best they can be.

AOL has been a leader in organizing industry efforts to educate consumers about on-line safety and is committed to continuing this leadership role. Among these efforts, AOL was a leading corporate host of the America Links Up national public education campaign, designed to give parents information to help their children have a safe, educational, and rewarding experience on line.

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

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

Finally, AOL works closely with the National Center for Missing and Exploited Children to support its mission of recovering missing children and to combat on-line exploitation of children.

Since July 1997, AOL and NCMEC have maintained an on line program called "Kid Patrol" which helps locate abducted and missing children. AOL also helped to launch NCMEC's Cyber Tipline.

In addition, AOL has developed a training video and a nationwide service of hands-on training seminars for law enforcement officers to teach their agencies how best to adapt traditional investigation and enforcement techniques to the on-line environment in order to effectively pursue and prevent cyber crime. We believe this type of cooperation with law enforcement and investigative organizations is critical to supporting AOL's on-line safety mission.

In addition to our leadership in industry efforts to educate families about on-line safety, AOL devotes significant time, energy, and resources to developing tools for parents to protect their kids on line. AOL's parental controls are the foundation of our child protection package and a key offering of our subscription service.

While providing kids with entertaining and educational experiences has always been an important mission for AOL, we strongly feel that it also our responsibility to help parents manage their children's on-line experiences. AOL's parental controls put the power in the hands of parents, enabling them to make informed de-

cisions about their kids' on-line activities by selecting the appropriate level of participation for each child.

Parents also have the ability to customize additional features, such as chat, E-mail, instant messaging, based on their children's on-line savvy, age, and maturity level. AOL's parental controls are server-based technology. This delivery mechanism means that the controls follow the child's screen names or E-mail address. So no matter where a child signs onto America Online, their parental controls will stay with them.

In 1998, we changed our registration process on AOL to require parents when creating a screen name to actually select one of four parental controls categories. The four choices are kids only, young teen, mature teen, or general access. Only master screen names can actually create a new screen name. That is the first screen name that signs up with the AOL service.

When creating a separate screen name for their child, parents can make the decision of what is right for their particular child. A kids only setting, which we recommend for children 12 and under, and there you will see actually those are the four choices that a parent is given just after creating a screen name.

If you select a kids only setting, this will limit access on line to the kids only channel, which has been specially created for children 12 and under. This child will receive a customized welcome screen when they sign on to AOL and it will have content that is specifically created for kids, both by AOL and by our kids' partners such as Nickelodeon.

A child using a kids only screen name can only access age-appropriate content on AOL and the rest of the Web. They interact in kids' chat rooms and message boards that are fully monitored by background-checked employees, who have been specially trained to work in these chat rooms and on the message boards.

In addition, by default, kids only screen names cannot instant message or visit any Web site that has not been approved as age appropriate. A parent could decide to turn instant messaging on if they so decided.

A young teen category, which is recommended for ages 13 to 15, provides more freedom than a kids only screen name, but does not provide full access to mature content and interactive features. Young teen screen names can access most AOL content and can visit Web sites that have been approved as age appropriate as well.

Young teens may communicate with others through E-mail and in a range of message board and chat areas, including our Teen Channel Chats and message boards, which again are monitored by background-checked and trained employees.

A mature teen setting, which is recommended for teens 16 to 17, allows older teens more freedom, but still a protected experience.

Each of these category settings has a pre-selected defaults for different features such as chat, E-mail, instant messaging, and Internet access. A parent, however, can choose to customize any of these defaults within a category to ensure the experience best matches his or her child.

So, for example, you could put your child on a kids only screen name, but you could choose a mature teen Web experience or you could decide that you do not want your child to chat at all, even

though you selected kids only. You could decide to block all AOL chat rooms even if they were monitored.

We continue to evolve our parental controls to meet consumer needs for safe, easy-to-use tools. In response to consumer request, we introduced our latest feature, the Online Timer, in the spring of 2000. This feature actually allows parents to determine how long and when their children can be on line and was among our most highly requested features.

We have found that education of our members is an ongoing process. As new consumers come on line every day and as our existing customers' lives evolve, their parental controls needs may change as well. AOL members spend an average of 76 minutes on line per usage per day; so we have ample opportunity to remind parents about their choices and about on-line safety.

We believe that every family should periodically review this new information, check their child's parental control settings, make sure they know their children's on-line friends, and update this information as appropriate as their child grows older and more mature.

We reach our members through several key vehicles on line. We have an area called Neighborhood Watch and parental controls, of course. These are our two on-line safety information areas. These areas are always available and they are promoted at a very high level to the members. In fact, the welcome screen has a button for parental controls.

We use keywords on AOL. We try to make them logical, such "child safety," "parental controls," "Note to Parents," and "help." These areas have lots of information and FAQs about how to make sure the child's experience is safe on line.

In our kids areas, our Kids Only Channel, and our Teens Channel, we have on-line safety tips designed for kids and teens. They are integrated into the experience. In fact, both children and teens must pass through these safety reminders before they may enter into a chat or a message board area. Every time they go in, they see the safety tips.

We also ask that our monitors in these areas remind kids if they see a child or a teen giving out personal information. The monitors have the tool to hide that in the chat. They also have the ability to gag a child or a teen or someone who is acting out in a chat room so that they are silenced or that they are actually evicted from the chat room.

In the kids help area we have on-line safety tips, and we remind kids day in and day out not to give out their home address, not to give out their telephone number, or any other identifying information.

We also have a special button called "Tell AOL" that is in the chat rooms. With one click a child or teen can notify us if they have a problem. Even though these chats and message boards are monitored, if they are in an instant message conversation, they can just go to keyword "Tell AOL." These reports now go into a special queue so that the member services representatives at AOL know that it is coming from a kids area or they know it is coming from a teens area and they can respond hopefully even quicker than they would in an ordinary circumstance.

To briefly summarize, AOL's commitment to families and child safety includes three elements: educating consumers about on-line safety; providing great age-appropriate content for young audiences; and offering parents easy-to-use, flexible tools to customize their child's on-line experience.

Finally, it bears repeating that at the end of the day, there is no substitute for parental involvement. Raising consumer awareness about parental controls, choices, and on-line safety is a collaborative effort. AOL believes that the industry and we have made great strides in this arena and are on the right path and continue to do so.

We look forward to working closely with you on this important issue.

Thank you again for this opportunity and I would be happy to answer any questions later.

[The prepared statement of Caroline Curtin follows:]

PREPARED STATEMENT OF CAROLINE CURTIN, DIRECTOR, CHILDREN'S POLICY, AMERICA ONLINE, INC.

Chairman Upton and Members of the Subcommittee, thank you for inviting me to testify before you today on issues relating to child safety in the online environment. As Director of Children's Policy for AOL, I am responsible for coordinating child safety and privacy protections across the AOL Inc. properties, as well as educating parents about online safety and the importance of parental involvement. I am pleased to have the opportunity to describe AOL's efforts to educate our members about online safety, the tools and resources we provide for our members—such as our easy-to-use, powerful Parental Controls—as well as our ongoing partnership with law enforcement and other stakeholders to help keep the online environment safe for children.

AOL has played a significant role in the development of the online medium and we have always shared a special appreciation of its enormous potential to benefit society especially children. Learning how to explore and understand the online world is an essential skill for our children in today's wired world, but we all agree that kids need and deserve special protection in this new medium. AOL recognizes that parents must have the ability to ensure that their children can enjoy a rewarding and safe interactive experience online. It has therefore been our challenge to craft rules of the road for children's online safety, enabling parents to protect their children while at the same time helping them take advantage of the wonders of the online environment.

By promoting major public education campaigns and closely cooperating with elected officials and government agencies on outreach and enforcement efforts, we have tried to offer strong proactive leadership in every area of children's safety online. In some ways even more important than those efforts, however, has been our commitment to providing our member families with the resources and tools they need to make informed decisions. No law, no technology, no corporate initiative can ever take the place of an educated and involved parent when it comes to their children's online safety. That's why we've dedicated significant energy to providing AOL parents with the most useful information, content, tools and safety tips to help protect their children, as well as a list of the resources available for families both on AOL and the Internet. By doing so, we've tried to empower parents so they can ensure that their children's online experience is the best it can be.

INDUSTRY EFFORTS TO EDUCATE THE PUBLIC

We have always believed that the industry must lead the charge in giving parents the tools they need to protect their children online. AOL has been a leader in organizing industry efforts to educate consumers about online safety and is committed to continuing this leadership role.

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

In addition, AOL created and distributed a special video for kids—called Safe Surfin'—that features online safety tips presented by some of the younger genera-

tion's favorite celebrities. This video was developed in partnership with the National School Boards Association and has been introduced into schools across the country.

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

AOL was also a key partner in forming the GetNetWise.org website—a resource designed to provide consumers with comprehensive online safety information that includes guidance from some of the major industry leaders, such as AOL.com, the AOL subscription service, and Netscape.

Finally, AOL works closely with the National Center for Missing and Exploited Children (NCMEC) to support its mission of recovering missing children and to combat online exploitation of children. Since July 1997, AOL and NCMEC have maintained an online program called "Kid Patrol" which helps locate abducted and missing children. AOL also helped to launch NCMEC's Cyber Tipline and has participated in an ongoing partnership to operate this service. In addition, AOL has helped develop a training video and a nationwide service of hands-on training seminars for law enforcement officers to teach their agencies how best to adapt traditional investigation and enforcement techniques to the online environment in order to effectively pursue and prevent cybercrime. We believe this type of cooperation with law enforcement and investigative organizations is critical to supporting AOL's online safety mission.

TOOLS AND RESOURCES FOR AOL MEMBERS

In addition to our leadership in industry efforts to educate families about online safety, AOL devotes significant resources to developing tools and resources for our own members to protect their children in the online environment.

a. AOL's Parental Controls

AOL's Parental Controls are the foundation of our child protection package and a key offering of our subscription service. While providing kids with entertaining and educational experiences has always been an important mission for AOL, we strongly feel that it is also our responsibility to help parents manage their child's online experiences. AOL's Parental Controls put the power in the hands of parents, enabling them to make informed decisions about their kids' online activities by selecting the appropriate level of participation for each child. Parents also have the ability to customize additional features such as chat, e-mail and Internet access based on their children's online savvy and maturity.

AOL's Parental Controls are a serverbased technology. This delivery mechanism allows us to provide the most secure experience to our members because the Parental Controls settings are actually attached to the child's individual screen name. No matter where that child signs online from home, school or a friend's house, the Parental Controls follow with the child's screen name.

In 1998, we changed our registration process to require parents to set Parental Controls for each screen name upon screen name creation. When we integrated Parental Controls into the Create A Screen Name process; we saw a dramatic increase in adoption as a result. There are up to 7 screen names available on one AOL account, enabling even larger families to give each child in the household his or her own screen name with customized Parental Control settings. Only "Master" screen names controlled by the parents can create a new screen name or set or change Parental Control settings.

When creating a separate screen name for their child, parents are given the opportunity to choose one of three different standard age "category" settings: Kids Only, Young Teens, or Mature Teens.

A Kids Only setting (recommended for 12 and under) restricts children to the Kids Only Channel, which has been specially created and programmed for children 12 and under. The child also receives a customized Welcome Screen. A child using a Kids Only screen name can access ageappropriate content on AOL and the Web and interact with others online through email and in special supervised kids' message boards and chat areas, but is blocked from taking part in general audience chat rooms and message boards on AOL, sending or receiving Instant Messages and visiting any Web site that has not been approved as ageappropriate.

A Young Teen (recommended for ages 13 15) category provides more freedom than a Kids Only screen name, but does not provide full access to more mature content and interactive features. The Teens also receive a customized Welcome Screen. Young Teen screen names can access most AOL content, and can visit Web sites that have been approved as age appropriate. They may communicate with others online through email and in a range of message board and chat areas, Including

Teen chats and message boards that are monitored by background employees. Teens are restricted, however, from accessing newsgroups, visiting inappropriate Web sites, or taking part in private chat rooms.

A Mature Teen (recommended for ages 1617) setting allows older teens the most freedom of any of the Parental Controls categories. Mature Teen screen names can access all content on AOL and the Web except sites that have been classified for an adult (18 plus) audience. They can locate others and communicate online through Instant Messaging, all chat areas, email, private messaging and AOL's Member Directory.

Each of these category settings has a preselected set of "defaults" for different features such as chat, email, Instant Messages and Internet access. A parent can choose to customize any of these defaults within a category to ensure the experience best matches his or her child so even on a Kids Only screen name (our most conservative), a parent may choose to further limit access to email to an "approved" list, or, alternately, may decide that the child is mature enough to participate in Instant Message conversations. A parent may choose to modify their child's access to content (Web, newsgroups, file downloads) or way to communicate with others online (e-mail, Instant messages, chat). For example, if you don't want your child to chat, you can customize Parental Controls and block all AOL Chat or you can choose only monitored AOL Chat.

We continue to evolve our Parental Controls to meet consumer needs for safe, easy-to-use tools. In response to consumer request, we introduced our latest feature, the Online Timer, in the spring of 2000. This feature allows parents to determine how long and when their children can be online, and was among our most highly requested features.

b. Educational Tools and Member Outreach

We have found that education of our members is an ongoing process. As new consumers come online every day and as our existing customers' lives evolve, their parental controls needs may change as well. AOL members spend an average of 76 minutes online per usage day (Source: Media Metrix March 2002) so we have ample opportunity to remind parents about their choices, and about online safety. This is important not only for new members to our service, but for existing parents as well. We believe that every family should periodically review new information, check their child's Parental Controls settings and update them as appropriate for that child's age and maturity. Also important, we have worked to quickly and effectively notify our members of significant news and developments in the area of children's safety, like the Children's Online Privacy Protection Act or new Parental Controls offerings that may impact their family's online safety decisions.

We reach our members through several key vehicles online. Neighborhood Watch and Parental Controls are our central "online safety" information areas. These areas are always available online to our members through easy-to-find mechanisms including:

1. **Keywords:** We use logical "keywords" such as "child safety," "Parental Controls," "safety," "Note to Parents," and "help" to lead our members to online education areas about child safety and privacy. Online safety for kids is a topic in our AOL Help AZ area. And we educate our newer members about keyword use early on, through Welcome Screen promotion of our Member Benefits Area.
2. **Prominent Placement:** Parental Controls is an icon on the Welcome Screen of our service which every member passes through each and every time they sign online. Additionally, Parental Controls are integrated into our Create A Screen Name process.
3. **Kids Only & Teens Channels Reminders:** Both our Kids Only Channel, directed to children 12 and under, and our Teens Channel, created for younger teens 13 to 15, have online safety tips integrated into the experience. In fact, kids and teens must pass through these safety reminders before entering interactive chat and message board areas. In the "Kids Help" area, AOL's "Online Safety Tips" remind children not to give out their home address or other identifying information to anyone online and to notify AOL and their parents if they encounter anybody that make that makes them feel uncomfortable or unsafe. There is a special "Tell AOL" feature that children can use to alert AOL of any such concerns.

An essential part of AOL's commitment to families, of course, is to provide great content for children. The AOL Service reaches over 3 million children ages 211 (Source: Media Metrics, March 2002). For almost 10 years now, AOL's Kids Only Channel has been delivering fun, engaging and educational programming to children 12 and under. In addition, all Kids Only chat rooms and message boards are monitored by background checked and specially trained AOL employees. And Yahoo!

Internet Life Magazine's 2001 awarded the Kids Only Channel the "Best Kids Community" for "kid-friendly games, chat and homework helpers."

CONCLUSION

To briefly summarize, AOL's commitment to families and child safety includes three key elements: Educating consumers about online child safety, including our collaborative efforts with other companies in the industry; providing great age appropriate content for young audiences; and offering parents easy-to-use, flexible tools to customize their children's online experience.

We are constantly enhancing our offerings to families and work closely with others in the industry to finetune our technological tools so that they are the most up to date and effective. Filtering, rating and labeling technologies are essential parts of the toolkit that can be used to protect children on the Internet.

Finally, it bears repeating that there is no substitute for parental involvement online. Raising consumer awareness about parental controls, choices and child online safety is a collaborative effort. AOL believes that the industry and we have made great strides in this arena and are on the right path to continue doing so. We look forward to working closely with you on this important issue.

Thank you again for this opportunity; I would be happy to answer any questions that you may have.

Mr. UPTON. Thank you very much.

Kathleen Tucker.

STATEMENT OF KATHLEEN TUCKER

Ms. TUCKER. Thank you.

Good afternoon. My name is Kathleen Tucker.

Thank you, Chairman Upton, for inviting me to testify today on behalf of I-SAFE America, a nonprofit Internet safety education foundation, and on behalf of our children who are at risk of predation upon on the Internet.

Predatory acts against children are among the most heinous of crimes that are perpetrated within our society today. With the technological advancement in Web tools that allow even the youngest of our children access to the Internet, a universal paradigm shift has occurred in the methods and means that are available to child predators as they stalk their prey. And as such, we need a universal paradigm shift to occur in the preventative tactics that we employ in an effort to keep our children safe.

I have had the opportunity to listen today to all of the other people who have testified before me, and I believe that the testimony that I offer will be complementary to that. I agree that parental supervision is key. I agree that law enforcement and the judicial process is key.

We also must be able to bring education as a tool, as a method of empowerment to those kids much in the same way that, as you spoke before, you do not just hand them the keys to the car and tell them to go drive. We do not hand them the keys to the information and access on the Internet.

Parents provide education and also we send them to school, where they are provided with education on driver's ed. or on gun safety, and then they are handed the tools with which to pursue those interests.

Chat rooms are among one of those technological advancements. Chat rooms, in and of themselves, are not inherently good or evil. They are electronically enabled methods for communication.

Unfortunately, one participant may use that method of communication to gain information about another participant for purposes of exploitation or entrapment.

There is no one solution for protecting our children. We need a well-balanced approach that attacks the child predation problem from a multiplicity of angles: education, economics, legal, and technical.

With respect to the value of education within this equation, I refer to a recently published study by the National Research Council and the committee to study tools on protecting kids against pornography and other inappropriate Internet content.

This study noted that an essential element for protecting children from inappropriate material on the Internet, and one largely ignored in this present debate, is the promotion of social and educational strategies that teach children—excuse me for just a moment.

Mr. UPTON. Thank you, again, to the Mattawon folks for coming. Thank you.

Ms. TUCKER. Thank you, Chairman Upton, for that short break.

Mr. UPTON. They have got buses to catch.

Ms. TUCKER. I understand.

Mr. UPTON. It is great that they could be here.

Ms. TUCKER. I thought I would give us all just a moment to let them file out and then I can continue.

Thank you again.

With respect to the value of education within this equation, I refer to this study. An essential element of protecting children from inappropriate material on the Internet and one largely ignored in the present debate are social and educational strategies that teach children to make wise choices and to take control of their on-line experience: who they meet, to whom they talk, where they go, what they do, and what they do.

Children need to acquire skills that will allow them to evaluate independently the information and images that they are viewing. By improving children's information and media literacy, they are better able to critically analyze those messages and images that they see and to be able to interpret underlying messages.

Children should be educated in Internet safety much as they are taught about their physical safety. This might include teaching them how sexual predators and hate group recruiters approach these young people on line.

They need to be able to recognize jargon that signals inappropriate material and whether to provide personal information.

To guide parents, public service announcements and media campaigns can help educate them about the nature and the extent of the dangers of the Internet and the need for safety measures. Many of our parents, many of the children's parents are not technically informed. They also need to be educated.

Just as our previous witnesses before have stated that they provide education with AOL on line, our parent here who has come forward to say that parents should be involved with their children, absolutely, and we need to get those educational messages out to the parents as well.

In conclusion, the value of empowering our children with the knowledge and critical thinking skills that they need to be able to independently assess the everyday situations that they will encounter while on line alone, without parents' supervision, they must have these through education. The children themselves must be able to effectively protect themselves against cyber predators. They must be able to recognize potentially harmful and inappropriate actions, to actively disengage from negative behaviors and compromising situations, and to seek help when they are threatened.

These lessons are learned. Education and empowerment are key.

Chairman Upton and Congressman Bass and other Members of Congress, you face a daunting task in initiating protective measures for our children, and you are to be applauded in this effort.

In I-SAFE America, we do offer our education programs and our outreach campaigns as one tool to be used with the many other tools that are available as you craft your solution.

Thank you for your concern, and thank you for your attention.

[The prepared statement of Kathleen Tucker follows:]

PREPARED STATEMENT OF KATHLEEN TUCKER, DIRECTOR, CURRICULUM DEVELOPMENT & IMPLEMENTATION, I-SAFE AMERICA, INC.

Thank you, Chairman Upton, for inviting me to testify before the House Subcommittee on Telecommunications and the Internet at the hearing entitled *Chatting On-Line: A Dangerous Proposition for Children.* As you requested, my testimony will focus on the dangers of Internet chat rooms to children and ways to educate parents and children about how to avoid such dangers.

Predatory acts against our children are among the most heinous of crimes perpetrated within our society. Historically, communities as a collective take deliberate and specific actions to protect their children in an effort to prevent these heinous acts. These protective actions include: education—teaching children to be wary of strangers, to recognize and avoid dangerous situations, to cry for help when they feel threatened; parental supervision—participation by parents in children's activities and the monitoring of the child's friends; preventative tactics—adult supervision at events when children are away from home; physical barriers—locking the doors at home, barring uninvited persons from access to schools and special events, keeping objectionable (pornographic) material in physical locations out of the reach of children; and, law enforcement intervention—prevention programs for students and the determent, apprehension, detention, and incarceration of persons known to prey upon our children.

With the technological advancements in web tools that allow even the youngest of children access to the Internet, a universal, paradigm shift has occurred in the methods and means available to child predators in pursuit of their prey; and, as such, a universal, paradigm shift must occur in the preventative tactics that we employ in our efforts to protect our children against these predators.

The content of my testimony today will address the ramifications of this universal shift, the dangers faced by our children as they explore the wonders of the Internet and as they interact in online Chat Rooms, the role of education and the need to empower our children in order to minimize the number of predatory acts predicated against them, and the criticality of a well-balanced approach that attacks the child-predation problem from a multiplicity of angles: education (children, parents, & the community), law enforcement, legal, and technical.

Let me begin by addressing specific examples of how dramatically the protective actions that have been employed historically have been impacted by this technologically-enabled, Internet-driven, paradigm shift.

1) *Education.* Parents teach children to be wary of strangers on the street, in public places, and at the front door; but now, the strangers that these children meet—are not on the street—they are in cyberspace. And, to the detriment of the parents, many of their children are more "Net" savvy than either parent. This inequality of knowledge hinders parents in their abilities to address cyber safety issues and to properly instruct their children about the dangers of meeting strangers online.

Historically, when parents taught their children to recognize and avoid dangerous situations, those situations were based on tangible, physical elements within their

community. Now, danger lies in an amorphous cyber-world cloaked in the allusion of anonymity.

2) *Parental Supervision.* Many of our children's activities have dramatically shifted from participatory activities (easily supervised by a parent and often enjoyable to watch) to solitary activities—engaged through the computer keyboard or joystick—that do not lend themselves to easy supervision nor enjoyment by a non-participant (such as a parent). Children may spend hours playing solitary games online, or they may play in tandem with their cyber friends, or they may even play with total strangers they connect with online in an Internet gaming community.

The Internet—and more specifically the advent of the Chat Room—has broadened a child's ability to meet other people and acquire "friends." Historically, children made friends at school, through family acquaintances, and from participating in community organizations. A child is no longer confined to the local community from which to socialize and gain friends; literally, cyberspace eliminates all geographical barriers and frees a child to roam the world in search of that one, special "friend." Predators are also free to roam.

The degree of difficulty for parents to monitor—or to simply meet—their child's friends has increased tremendously.

3) *Preventative Tactics.* A commonly employed tactic for protecting our children is to provide an adult chaperone as our children explore outside of their community. Now, children explore the wonders of the world by transporting themselves through cyberspace. They can travel to the brightest, most intellectual domains of the universe and, conversely, they may travel to the darkest, most detestable realms of the human imagination; and, they travel this world alone, without the care and protection of a chaperone.

4) *Physical Barriers.* Historically, parents routinely lock their doors at home each night to keep intruders out; schools monitor persons who enter the campus; and objectionable (pornographic) material is distributed from adult-only sections in local businesses. Presently, parents continue to lock their doors, but, their children inadvertently invite the pedophile into their bedrooms through a chat room conversation or via email. Gone are the days when predators have to search for unlocked doors or open windows. Gone to are the days with the child predator had to troll the schools or neighborhood playground to find a child that is isolated, or lonely, or bored; all the predator has to do now is to troll the Internet. There are innumerable, vulnerable children who are isolated, and lonely, and bored who constantly search the Internet for other children with whom they can make friends and chat. As these children search the web for friends so too the predator searches the web for prey. The predator will find the child, the child will find a "friend,' and the outcome will be devastating.

The effectiveness of currently employed physical barriers has been severely compromised. Predators lure and seduce their victims from within the privacy of the victim's own home. Pornography intrudes into a person's private email and appears on the screen when a child inadvertently selects a pornographic website while conducting research for a homework assignment. Predators, pornographers, pedophiles, operate in a world that is no longer constrained by physical limitations or geographical barriers; they stalk their prey through cyberspace and routinely visit their prey as invited, virtual guests into the home of their next victim.

5) *Law Enforcement Intervention.* As Internet use continues to grow, so will the number of cyber criminals. These criminals are sexual predators, pornographers, hackers, and thieves. They target and then victimize innocent people—especially our youth and our elderly—via this electronic highway. Crimes vary from theft of credit card information or personal identities to solicitation of sexual acts, stalking, hacking, and trafficking in child pornography. Many of the crimes are new (computer hacking for example) while other crimes, such as child predation, have haunted law enforcement officers for centuries. Regardless of the nature of the crime, the criminal's method of attack—via the Internet—is relatively new; the Internet has changed the rules of the game. Given that the methods and means employed by predators in their victimization of our children have changed, so must the tools and techniques employed by law enforcement in the pursuit and apprehension of these predators. Law enforcement must be allowed to leverage the same technological advances that the criminal element uses. Without these advanced tools—law enforcement is handicapped. And, given that the methods and means employed by predators have changed, new community prevention programs that are taught by law enforcement must be developed to inform and advise our citizenry of new protective measures.

The ramifications of this universal, paradigm shift are staggering. If taken as a whole they can be overwhelming, perhaps paralyzing; but—if ignored—the ramifications will be devastating to our youth. To approach any entity of this magnitude and

to effect change it is advisable to search for a common element, theme, or component against which a focused solution may be enjoined.

One common and persistent theme, that has tentacles into every aspect of the aforementioned points, is the chat room.

Today, I will focus on the dangers that unsuspecting children and youth may face while engaged within a chat room and the subsequent dangers they may face as a result of their activities in a chat room. This focus, this perspective, is for the purpose of this testimony only and is not intended to discount any of the benefits that may be gained through dialog among participants within a chat room nor is it intended to discount the benefits that can be gained through the healthy exchange of ideas and information. Chat rooms are not inherently good or evil; they are electronically-enabled methods of communication that, unfortunately, can be used by one participant to gain information about another participant for purposes of exploitation or entrapment.

As defined in *The American Heritage*® Dictionary of the English Language, Fourth Edition, Copyright © 2000 by Houghton Mifflin Company, a chat room is: "A site on a computer network where online conversations are held in real time by a number of users."

How does this seemingly innocuous entity, a chat room, play a major, insidious role in the entrapment and exploitation of our youth?

Let's explore the answer to this question by overlaying the influence of the chat room on our new cyber paradigm. A chat room is a smorgasbord; it is: a town centre—a meeting place for debate; a coffee shop—a place for chat and banter; a celebrity hangout—where people can chat with their favorite musician or star; a club—where like-minded persons discuss common interests; a playground—where kids hang out with their friends; and, an unprecedented opportunity—where persons from anywhere in the world can gravitate to meet new "friends," exchange ideas, and communicate.

Children participate in chat rooms every day so that they exchange ideas and information, they can hang out with their "friends" and they can actively search for new friends. Last week, as I taught an Internet Safety class to a group of 6th graders, I posed the question: "Do any of you have a cyber friend that you met online that you never knew before?" Several of the students raised their hands. I asked one young girl to tell the class about her "friend." She said that she was bored and lonely so she went online into several chat rooms specifically looking to find a friend. She said that she found one and they quickly discovered that they had a lot in common. I asked her what they chat about. She replied: "Everything." She said they talk about family, sisters, brothers, parents, pets, school, where they live . . . Literally, the hairs on the back of my neck were standing on end. I asked her how she could trust a stranger with so much information. She said that she doesn't feel like this is a stranger, this is her friend, and she "knows" that her friend is a child—not an adult—because her friend "knows too much about things my age—and there's no way that my friend is an adult pretending to be a kid—it's just not possible."

This child is a cyber-savvy pedophile's dream-come-true.

The paradigm and the chat room:

1) *Education.* Parents teach their children to be wary of strangers; but, children don't view their online "friends" in the same way as they view a stranger on the street. They haven't made the tangible association between their physical world and the cyber world. In their own mind they envision what they believe their friend "looks" like, and no child is going to envision their cyber friend as old or threatening.
2) *Education.* Children are taught to recognize and avoid dangerous situations. They recognize places within their physical community as potentially dangerous but have not learned to recognize the potential for danger within the chat room.
3) *Parental Supervision* & *Preventative Tactics.* Children rarely "travel" with their parents or a chaperone to many of the chat rooms where they hang out. Without education to raise their awareness and to empower them to recognize the danger of being alone in a room full of strangers, these children are at risk for exploitation. In July 2000, The Journal of the American Medical Association, in cooperation with a survey that was conducted by the University of New Hampshire's Crimes Against Children Research Center, published a "Call to Action Report" in which it reported that girls, older teens, troubled youth, frequent Internet users, chat room participants and those who communicate with strangers online are at the greatest risk. The study also confirmed that children often don't understand the risks associated with talking to strangers online *(David Finkelhor, Director of the University of New Hampshire's Crimes Against Children Research Center).*

4) *Physical Barriers.* Chat rooms eliminate the physical and geographical barriers that used to provide a modicum of protection to our children from the predatory elements of our society. Pedophiles now roam the world, without limitations, in pursuit of their next victim. A case in point is the recent seduction of a 13 year-old girl in Katy, Texas who was lured from her home by a 34 year-old pedophile—who she met in a chat room—to his apartment in Tacoma, Washington. This sexual predator allegedly exchanged pornography with his victim over the Internet, arranged transportation to take her from Katy, TX to Tacoma, WA, and raped her over a five day period of time.
5) *Law Enforcement Intervention.* Chat rooms pose special challenges for law enforcement as well. These hunting grounds for child predators are now the patrol beats for specialized officers in pursuit of these criminals. Technology has wrought dramatic change for both the offender and the officer.

Up to this point in my testimony, I have provided insight into the incredible, paradigm shift that has occurred in our society and how this new paradigm directly affects the safety of our children. To exemplify the critical points, I mapped the ramifications of this paradigm shift to a common element in cyberspace: the chat room. The remainder of my testimony will focus on potential solutions that we as a society may embrace in an effort to combat the clear and present dangers that our children face as they explore the farthest reaches of cyberspace, as they interact, virtually, with persons throughout the world, and as they evolve as "Net" citizens.

As Judith F. Krug, Director of the American Library Association's Office for Intellectual Freedom, stated in her testimony before the COPA Commission on August 3, 2000: "The children of today will be Net citizens for the rest of their lives. They need to be taught the skills to cope in the virtual world just as they are taught skills to cope in the physical world. Children should be educated in appropriate increments and appropriate settings on how to avoid inappropriate Internet content, to report illegal or unsafe behavior and to engage in safe interaction online. Children who are not taught these skills are not only in danger as children in a virtual world, they also will grow into young adults, college students and an American workforce who are not capable of avoiding online fraud, Internet addictions and online stalking."

Our children now live in two diverse worlds: their physical world and the world of cyberspace. As such, they essentially live in two cultures that often conflict. To date, many of the lessons learned in the physical world don't seem relevant in cyberspace as these children reach out to strangers as friends. This paradigm shift demands new, innovative educational programs for our children, their parents, and the community. It is essential that children, as they travel their world of cyberspace alone, be provided with the knowledge they need: to independently recognize and avoid dangerous situations online; to actively engage learned, proactive techniques to more safely interact with strangers online; to critically appraise situations in which they find themselves; and, to react appropriately when they find themselves in uncomfortable, compromising, or threatening situations.

According to a press release on May 2, 2002 published by the NATIONAL RESEARCH COUNCIL, Division on Engineering and Physical Sciences Computer Science and Telecommunications Board and the INSTITUTE OF MEDICINE, Board on Children, Youth, and Families regarding the findings of the *Committee to Study Tools and Strategies for Protecting Kids from Pornography and Their Applicability to Other Inappropriate Internet Content* (chaired by Richard Thornburgh):

> An essential element of protecting children from inappropriate material on the Internet—and one largely ignored in the present debate—is the promotion of social and educational strategies that teach children to make wise choices about using the Internet and to take control of their online experiences: where they go, what they see, to whom they talk, and what they do.
>
> Children also need to acquire skills that will allow them to evaluate independently the information and images they are viewing. By improving children's "information and media literacy," they are better able to critically assess material, recognize underlying messages, and locate the information they seek.
>
> Children should be educated in Internet safety much as they are taught about their physical safety, the report says. This might include teaching them how sexual predators and hate-group recruiters typically approach young people online, how to recognize jargon that signals inappropriate material, and whether to provide personal information. To guide adults, public service announcements and media campaigns could help educate them about the nature and extent of dangers on the Internet and the need for safety measures.

Education is a critical and essential component in combating the threat of child predation via the Internet; but, it is only one element of the solution. To stem the online predation of our children, it is essential that a multiplicity of elements be

collectively engaged as part of an overarching solution: education (children, parents, & the community), law enforcement, legal, and technical.

According to the National Academies' National Research Council report noted previously (this report is available in its entirety online at www.nap.edu/books/0309082749/html): No single approach—technical, legal, economic, or educational—will be sufficient to protect children from online pornography. I believe this statement can be extended to include all aspects of predatory acts perpetrated against children online. The report goes on to describe the need for social and educational strategies, technology-based tools, and legal and regulatory approaches that can be mixed and adapted to fit different communities' circumstances.

There are many technology-based tools that are currently employed in an effort to protect children from exposure to offensive or pornographic material online. These tools include filtering and the blocking of websites that may potentially contain offensive materials. A heated debate surrounds the use of filtering and the constitutionality of these and other similar tools. With respect to my testimony and the use of technology to provide increased safety, I will recognize that filtering is one of a set of tools available and I will focus my testimony on a different technology-based tool that may potentially prove to be a powerful enabler to the managers of chat rooms for attaining "best effort" policies and procedures for protecting children who frequent their chat rooms: digital certificates.

Currently, both businesses and governmental agencies have begun to embrace digital certificate technology as an electronic means for identifying participants in transactions that occur online. They leverage this technology as a method for verifying and authenticating a person's electronic identity. The simplest way to view a digital certificate is as an electronic ID card. However, digital certificate technology is far from simple; but, given that the intent of this testimony is to identify and express how technology can be used, rather than to define the intricacies of the technology, I will refer to digital certificate technology in the simplest terms possible for the reader to understand. For anyone interested in garnering a more in-depth view of digital certificates and digital signatures you may want to visit the American Bar Association, Section of Science and Technology, Information Security Committee website to review the document *Digital Signature Guidelines Tutorial* (www.abanet.org/scitech/ec/isc/dsg-tutorial.html).

Digital certificates are issued by a certification authority. A certification authority can issue various levels of digital certificates that are dependent upon the amount of authentication that is required to ensure that the person who is applying for the digital certificate is in fact the person that he or she claims to be. In other words, to obtain a digital certificate a person must present proof of identity and the "level" of the certificate obtained depends upon the amount of proof required.

Example: Acme Certification Authority
Level 1 certificate—any photo ID required
Level 2 certificate—government issued photo ID required
Level 3 certificate—government issued photo ID required plus passport or birth certificate
Level 4 certificate—all requirements of Level 3 plus a background check
Level 5 certificate—DNA

How could digital certificate technology increase the safety of children who frequent a particular chat room?

A public- or private-sector chat room provider could engage digital certificate technology as a means for permitting or denying access to any given chat room. Conceivably, a chat room provider could institute a policy that only children under the age of 13 are allowed to participate in a particular chat room. The intent of this policy is to provide a safer online environment by making their "best effort" at excluding adults and potential pedophiles from the chat room. To enforce the "under the age of 13" policy, the chat provider would require all participants to login using a Level 3 digital certificate. Through the use of the digital certificate and the chat provider's policy of restricting access, the children participating in this chat room have a lessened degree of risk than those children that participate in unrestricted chat rooms.

This technology exists. We currently use it to execute online financial transactions. Businesses use this technology to protect their monetary assets; perhaps, we should explore how it can be used to protect our most precious asset: our children.

Protecting our children is at the very heart of this hearing. Thank you, Chairman Upton, for inviting me to testify before the Subcommittee on Telecommunications and the Internet. In my testimony, today, I addressed the paradigm shift that has occurred within our society due the advancements in web technologies and the advent of chat rooms; exposed the dangers our children face online and the difficulties

faced by parents in protecting our children; touched upon one technological approach for increasing the abilities of chat room providers to create safer chat room environments; and, most importantly addressed the importance of education in protecting our children from falling victim to online predators.

In conclusion, there is no one solution for protecting our children. However, the value of empowering our children—through education—with the knowledge and critical-thinking skills that they need to be able to independently assess the every-day situations they will encounter while online cannot be overstressed. Children must be able to effectively protect themselves from cyber predators, to recognize potentially harmful or inappropriate actions, to actively disengage from negative behaviors or compromising situations, and to seek help when threatened. These lessons are learned. Education and empowerment are key.

Mr. UPTON. Thank you all. I know Charlie and I have a number of questions, and as I said before we started, I want to make this more of a dialog than a formal give-and-take, courtroom type scene.

You know, as I think about this, obviously I think first as a dad. I have got a 10 year old and a 14 year old. I also serve on the Education Committee, and like Charlie, I probably visit schools virtually every week, all different levels, from college like here at KBCC to elementary school.

And one of the things that I have been doing over the last 6, 8 months, particularly as my role as chairman of the Telecommunications and Internet Subcommittee, has been focusing on elementary school students, knowing that I have got one that is ten, and just looking at the changes in technology that he has gone through versus where my daughter was 4 years ago. And it is just an incredible change.

I know two devices connected to the Internet today, talking about the explosive growth. One hundred and fifty million devices today are connected to the Internet. By 2006, it will be a billion devices worldwide connected to the Internet. So they will be in our cars, on our wrists, in our offices, our homes, you name it.

And with that comes that double edged sword, and with the growth of technology, the dangers, the nightmares that are out there: Katie's story, John's story, Jim's story about what is happening here in Kalamazoo.

But when you tie that to what Ruben indicated, usually perhaps as many as 30, 100 children before you get a conviction? Three hundred children per molester is about the average.

I mean, I think of this gentleman this week that you are going to be pressing charges against, a 34 year old. And just think how many families.

Mr. GREGART. We have 20 additional names of females that were seized from his computer that we are following up on now.

Mr. UPTON. That is just a pretty scary feeling.

Charlie.

Mr. BASS. We have heard some interesting stories and some possible solutions. As a Member of Congress, I would like to know exactly what recommendations you have or suggestions for action that we might take on the policy level. I have not heard anybody discuss that.

Mr. UPTON. I have just one idea first, and then I want to hear the response.

You know, I wear two hats, sit both on the Education Committee, as well as on the Energy and Commerce Committee. As we look at education legislation, you know, my brother is a teacher, and we

visit schools. It is so hard often to get parents involved to oversee exactly what is happening.

You cannot legislate parental involvement. I know that, but I wonder what incentives we might be able to do working with our school boards, our schools at every level to make sure that parents, in fact, get a daily dose of the dangers that are out there to try and make sure that they're engaged, looking over their kids' shoulders.

Do you have AOL?

Mr. BASS. Me? No.

Ms. CURTIN. We can provide you with a disk.

Mr. UPTON. Yes. I think you can get them at the A&P.

Ms. CURTIN. That is reassuring.

Mr. BASS. Again, Mr. Chairman, if I can reiterate though, we make policy, and this is a very serious and interesting problem, but precisely what suggestions do people have for us, policymakers?

If you were to draft a bill, what would it say?

Mr. GREGART. If Congress were to recognize that this is a public safety issue similar to automobile collisions and the mandate for airbags and crash worthy vehicles, the issue is: how far does the Federal Government want to put its hand into technology and manufacturing?

But I probably would have found it helpful if there were a CD not just offering AOL for the first 1,000 hours when I bought my new computer, but a CD that was clearly marked as educational material prefatory to allowing children access to the Internet or bundle it with the software for the different programs that come with a new computer.

What do I have now, AOL 7.0? Is it 7.0? Well, it started off with AOL 0, I think.

And every time AOL has upgraded, I have gotten the next version. So I probably miss a lot of the new things, but when you open a new computer, if you had just a singular CD, which costs how much to burn? Not excessive, but it was clearly marked as a condition precedent for you signing onto AOL or any other ISP, just like airbags in automobiles.

Ms. TARBOX. I like to tell this story because it does not take too long and because I think it relates well.

I personally never thought I was going to be a victim of AIDS, and I had a speaker come to my school, and she was from the town next to me, and she was with her boyfriend, and he was cheating on her, and he gave her AIDS. She goes to Harvard, and I could see myself, and I could relate.

And through that story I realized I am just as much a victim. I mean I could be just as much at risk as any other person.

I think the problem is that people think if they start chatting with somebody on the Internet that their case is different. They are not the case like they just heard from mine. And people need to realize the dangers.

And I think the best way to do that is to go out and educate. And I know that the government is mandating when the government provides funding for computers for schools. They should provide funding for education. Children need not to be told statistics that

are going to go in one ear and out the other. They need to be told stories that they can relate to.

And I think education is so key because the education is going to go with that child wherever they go, and while I think it is important that we do monitor chat rooms and whatnot, that is only going to be limited to that computer. If we give them education and the tools to be empowered on the Internet, that is going to go with them everywhere.

So I think there needs to be funding for or laws that require if you are going to give them a computer in the school, then they need to know how to use it. And those dangers are out there, and there are consequences to them.

Mr. UPTON. Before we jump over here, let me just say, too, as I talk to my kids and students at school, peer-to-peer discussions are the very best in terms of trying to influence or trying to get your message across. And that is why, Katie, I think your story relates so well, you know, to everybody in this community, and that is why I wanted a public hearing here to help identify problems and, you know, get those stories across so that everyone here can hear exactly that.

And perhaps from this there will be a lot of families that will sit down here tonight when they watch the news or read the paper or listen to the radio, conversations from the students who were here a little bit earlier, and they will just say, "Boy, did you hear what I learned today?"

And that will open up a whole new chapter in that family's house and neighborhood and help try to spread that message.

Ms. TUCKER. In the education formats that we found most effective are when we do present real life stories much like Katie's, and what is important is that the children are not just frightened. You know, you do not just give them horror stories, but you give them examples, and you allow them to be able to work with those examples in peer groups in the room and come back with ways that they can empower themselves to protect themselves or to recognize what those dangers were.

I listened to a young girl the other day, which scared me to death. I was teaching in a sixth grade class, and I asked all of the kids if they were involved in chat rooms, and most of all of the hands go up.

And I said, "Have you ever met a cyber friend that you never knew before?"

And this little sixth grade girl raises her hand, and I call on her, and I said, "Well, what do you talk about?"

And she says, "Well, everything."

And I said, "Well, why did you meet this friend in the first place?"

She said, "Because I was lonely."

And I said, "Now, when you talk about everything, what does that mean?"

She says, "Oh, my family, my school, my sisters, my brothers, our pets, where we live, what we do, what we like."

And I said, "And you trust this person?"

And she says, "Oh, yes, I trust this person. I know it is not an adult because this person knows too much about what a sixth grader likes. No adult could ever know that."

So what we do in these classrooms, of course, is provide examples, you know, like Katie's of how they do know or this gentleman who testified today about his daughter, you know, trusting this person.

And we let them realize what a true friend is, what trust should be, and then we provide these examples so they can understand the difference and make critical decisions because they are going to make those decisions in lieu of parental supervision also. And I do not discount parental supervision whatsoever. I agree that there are many tactics that we need, and that is one of them.

Mr. UPTON. Caroline, before you answer, I would like you just to comment on the steps. You talked about you are able to monitor somebody's chat. Describe exactly how that works and some of the things that you have found in addition to responding to the same topic.

Ms. CURTIN. Oh, certainly. Well, basically in our kids only area on AOL, it is literally impossible to open a kids' chat room or go into a kids' chat room unless a host or a monitor has officially opened the chat room. The chat rooms are not open 24-seven. They are on a schedule. There is always a monitor who is identified as the monitor in the chat room, and he or she is not only there to help insure that it is a safe interaction, but also that the conversation remains relatively age appropriate.

One thing that we did a year ago or so because the chat room dialogs were getting a little bit rambunctious, to keep it PG so to speak, was we instituted a stop sign before the interactive areas. I mean it is literally a red stop sign, and we say to kids and teens, you know, "Keep it clean. Do not give out your person information. We want everybody to have a great experience, and just FYI, if you do not, we will be sending a letter or an E-mail to your parent."

That worked really well, and what happens is if three E-mails go to the parent, we literally scramble the parent's password on AOL so that they cannot sign onto AOL without first calling in and speaking to a member services representative of AOL about what has transpired, about our guidelines in our kids and teens areas and the importance of on-line safety.

So that as proven to be very effective, but I think what we are hearing over and over again is kind of a three-pronged approach, a simple equation, so to speak, for on-line safety: one being empowerment both for parents having the resources and the tools and the education, and for kids to know what to do, what to look out for.

Two, education, baking it into the curriculum of the school that has Internet access; really reaching out to the kids, telling them real life stories.

I would agree. I was at a middle school a few weeks ago, and I made the mistake of having a quiz, and I handed out AOL tee shirts, you know, if the kids answered the quiz correctly, and they went crazy, and I could barely get them back. I could barely get their attention back, but what stopped them was a real life story of a man that worked for a computer associate firm, and it was an

on-line stalking case, and the room went silent. And that is what caught their attention, and then their hands went up, and they really wanted to know what to do to stay safe.

And then the third is enforcement. And we fully support greater resources, greater education, stiffer penalties for pedophiles. So I think it really is those three Es in a nutshell.

Mr. UPTON. Kathleen.

Ms. TUCKER. I had a question along the lines of your chat rooms. Can you guarantee that a participant in a chat room is a child?

Ms. CURTIN. No, we cannot. There is no way for us to know that definitively without asking for someone to come and meet us in a brick and mortar setting really. But that is why we have the monitors there. That is why they are trained.

They are trained to look for people that might be acting as if they are children, asking inappropriate questions. We do say that the kids and teens chat rooms are attended for kids and teens.

In addition, if a parent wants to use our tools, they can really fine tune the chat experience. They can also block instant messaging entirely. They can block E-mail.

If they do not want to do that, they can create an allow list of kids' friends, family members that they do feel comfortable with their children talking to and limit it that way.

Mr. UPTON. If you do an allow list and Johnny down the street is on there, but Johnny has got another friend, is he able to pull in somebody else or not?

Ms. CURTIN. He is not.

Mr. UPTON. It will just be a strict one.

Ms. CURTIN. It is a strict allowance, yes.

And we also have instant messaging controls for kids or any user on AOL so that if someone is bothering them, they do not want to talk to someone anymore, they can put that person on their black list. They can also make themselves invisible so that the other person cannot have them on their buddy list and see that they are on line.

Ms. TUCKER. And the reason that I ask those questions, have you considered digital certificates?

Ms. CURTIN. We have looked at digital certificates. I think there have been great advancements in technology across the board, but we have not seen digital certificates take off to the point where we have reached critical mass so that they will really be effective, but we are hoping that they get there.

Ms. TUCKER. We are going to pose this just as a thought for you as you move forward. One other technical possibility for a solution is the use of digital certificates, and for those who are not familiar with digital certificates, I am going to say it very simply. They are electronic ID cards, and you get these by going to a certification authority who has different levels, but allows you to perhaps show a photo ID or even a birth certificate.

If we think out of the box a little bit and we were to think about in the future issuing digital certificates for children who were at school because those certificates would be guaranteed and the fact that a child attending a school has presented a birth certificate, you know, is identifiable, and perhaps we were to use those digital

certificates within chat rooms, perhaps your dot-kids domain, it may be able to help to protect the area from predators.

Mr. UPTON. John had a comment.

Mr. KARRAKER. We are talking a lot about AOL. We need to recognize there are hundreds of Internet service providers, and we are not addressing the industry as a whole. It sounds like AOL has changed a lot of what they do since I last dealt with them, but I really think there should be some industry standards of what should be done by the industry on the Internet as far as monitoring chat rooms and what have you.

But we also need to look at I do not hear a lot of conversation about instant messaging that says AOL's, IM, Microsoft, Yahoo. All of the rules are downloadable, free, instant messages services that nobody monitors.

A child can come home to an empty computer, go on line with whatever service you may be using, download AOL as an example, have all of the IM they want to do while I am not home. Before I get home they can delete that whole thing, and I never even know they have been on the computer.

I am not the technical expert to talk about it, but really it needs to be addressed within the industry with oversight to develop some type of controls on this type of stuff.

We can talk all about chat room controls, but we are only addressing a small part of the problem.

Mr. UPTON. But, you know, as Charlie asked the question of what can we do as legislators to help, we work with the Department of Commerce and other different agencies. I wonder if there might be some code that could be established, Good Housekeeping Seal type of thing, that Internet service providers if they follow that course would be able to achieve that particular distinction as a help, whether looking first at the industry, trying to establish a code that has got some teeth in it.

We both worked very hard to establish dot-kids with ICANN, you know, like we have dot-org and dot-com; have a dot-kids. The national folks, you know, a day late, a dollar short, too late. And that is why we went to a different little version of that so that it is actually dot-kids-dot-U.S., under the auspices of the Department of Commerce set up through the private sector.

And my sense is that that will take off, particularly as parents learn about those sites and tell their 10 or 11 or 12 year old that they are welcome to get on the Internet, but it had darn well better be a dot-kids site and a lot of different groups then funnel in as part of that exercise.

Ruben, did you want to comment on that?

Mr. RODRIGUEZ. And I agree with John that we have been talking about the industry in general, but one of the things we have not talked about is the IRC, very unregulated, global medium. You access it through your ISP on the Internet. Thousands and thousands of chat room and channels are open for communications.

Many of these cases that do occur do not occur in the environment of AOL. Some of the cases we have talked about here did, but the majority of cases are happening on IRC where you do not have monitoring. You have no controls.

Somebody creates a channel. Communications are done. If you got into IRC right now and you type in "sex," you will probably get about 1,100 conversations going on right now in different chat rooms going in communications. That is where the pedophiles are. That is where the kids are going to look because the controls are not there.

You are also talking about what can Congress do. Well, Congress has been doing a lot. I mean, give yourselves some credit here. You funded initiatives like the school resource officers training program that is similar to the DARE program, where you are empowering and educating law enforcement officers to go into the schools and talk about this.

And as they did with drugs with the DARE program, now they are talking about Internet safety issues.

I do agree with you that when you talk to the focus groups about kids, who will kids listen to? They will listen to their peers. We are currently doing a program called Net Smart, a proactive interaction between our Web site, chat rooms, and whatever, with kids.

Kids will listen to kids. We ask them, you know, if we were going to sell this idea to you, who would you listen to. Would you listen to the Michael Jordans of the world or anybody else?

They said, no, because they are getting paid, and we know they are making high dollars, but we will listen to kids, not demeaning Katie, but kids that have done this, that it has happened to them.

Katie is probably one of the older people now in this group, but I mean people that have experienced it. War stories. And I do agree. The public can relate it to war stories, as policemen used to call it. Tell us a story and that way it will relate it to us. Do not give us the technical jargon or whatever, but tell us, you know, how will it affect us. What will it do to us or whatever?

So Congress has been putting laws into effect to help this, and they have been empowering law enforcement officers' educational programs.

I made the mistake about a year ago going to a PTR seminar where in the State of Virginia I did a presentation. And after the presentation, I had 33 invitations within about 2 weeks to go present in these schools, and there is no way one individual can do that.

Educating those that are at the local level, as I said it before, and I might sound like a broken record; educating those resources that you have at the local level, your law enforcement resources, your continued relations law enforcement resources to outreach to the public, to go into the schools.

At one time we thought about educating teachers, but in defense of teachers, they have so many responsibilities they have to deal with now. You have to bring people from the outside to be able to talk about these things, and I think the people that are there doing the outreach, the education are the law enforcement officers going into the schools at the local level. That I think are where the resources need to be Ms. CURTIN. Just to respond to the comment about instant messaging programs and there being certain other ISPs besides AOL, we agree. We do not want to be alone in this. You know, it needs to be an industry-wide effort clearly, and there has to be strong collaboration.

I mean no one person, no one company can do it on its own, and with respect to AIM, that is our free instant messaging service. We do not recommend that for children. We, in fact, have an age screening mechanism on AIM so that birth date and year is required. It is not allowed for children 12 and under.

That is not foolproof if a child decides to fudge his or her age.

Mr. UPTON. Foolproof in my house.

Ms. CURTIN. Good. There are ways to get around it, of course, as there are anything. I do not think that we are ever going to, you know, be able to block or shut down all of the instant messaging programs. I think it gets back to education, again, and how kids and teens can be equipped when they are using these mechanisms because the fact is that is how kids and teens communicate these days, and that is just the reality of it.

So we do have tools on AIM even for blocking people, for actually notifying us if there is a problem. You can warn someone on AIM, and if you are communicating with them, you can actually see how many warnings does this person have, which is an early indication that maybe it is not such a good person to be talking to.

We also have something that we call a knock-knock feature on AIM. So if you are on AOL and someone instant messages you from AIM, a box comes up and says, "Would you like to accept this instant message?" It is not just all of a sudden you are talking to Horselover at AOL.

So there are protections in place, but it is also a free service. So we do not have as much leverage as we do on the subscription service, where we know who the subscriber is and we have their address and we have their credit card number. If we get a report, we can really do something about it.

Mr. UPTON. Katie.

Ms. TARBOX. Just to get back to the documents because I think that is probably a large reason why we are here today, I agree with all that we have been talking about. I do not feel that there is one solution.

But when I first heard about the dot-kids bill, I was kind of hesitant because I thought, you know, this is not the answer. They need to do something more.

But then as I started to think about it, and I am lucky enough to be able to take courses at the Edinburgh Public Policy Center at the University of Pennsylvania in Philadelphia, and anyone who knows media communication, these are probably some of the leading professors and researchers.

And speaking with my professor, who is a specialist actually in the Internet safety for kids and other Internet related issues, and I think that it is important that this legislation outlines that the content on these Web sites, specifically dot-kids, is going to be appropriate because this will be most children's introduction to the Internet.

Most parents will probably put on their Internet filtering software and allow it to be just in the dot-kids area, and so, therefore, I think it is important that the legislation clearly lays out, you know, what kind of Web sites are going to be allowed and so that kids learn that the Internet is for information, for doing homework, for communicating with people that they already know, and looking

at it like that, and not having the introduction like I had where it is like a bar. You go to meet people.

Mr. UPTON. That is exactly what the intent is on the dot-kids, to do exactly what you just described, and it is going to be the introduction, and they will learn a whole number of skills, and as they mature, they can still stay on it. They will obviously be able to select other sites as well.

I want to come back, Caroline, just to ask: how hard is it for folks to somehow disengage?

My 10 year old is very responsible, a proud dad. He is not going to do that.

Or he will lose a lot of privileges. But how hard is it for someone to go around and, in essence, hack into the sites that you have otherwise thought you have blocked off from your son or daughter?

Ms. CURTIN. On AOL it is very difficult, and that is because it is a server based technology. So that as I referenced earlier literally the screen name for your child is attached to the parental controls. So as we do see more and more devices, palms, and blackberries and AOL TV and all of these different ways that you can access the medium from home or away from home, no matter where you are, if you as a parent have applied parental controls to that screen name, they will always be in effect.

But no system is perfect. Let me say that. No system is 100 percent infallible 100 percent of the time, but these are pretty close.

Mr. UPTON. Jim?

Mr. GREGART. By lack of fallibility, do you mean that if I were to buy a new account as an adult with a credit card and then sign up my fictitious children with parental controls attached to them, then that you would not know that if I went in under one of the names of my disguised, alias, fictitious children that, in fact, I was not a 60 year old?

Ms. CURTIN. We would not know that. When a parent or anyone creates a screen name, we do not ask how old is the person you are creating this screen name for Mr. GREGART. So you would know what age level I had set it at. So there would be sort of a predisposition that, you know, Goofy Jimmy or whatever my key name is——

Ms. CURTIN. Actually we would know on the back end, but let's say that you went into one of our kids only chat rooms or the teens chat rooms and you had a parentally controlled screen name. We would not know that just on the surface of things, and no one else would either.

And one of the things that we have tried to do is really make sure that in our kids environment, our kids channel and our teens channel, it does not matter if you are on a parentally controlled screen name or not. We have the same policies for safety and content in place because not every parent is going to choose to apply parental controls.

Mr. UPTON. But if somehow you went to the digital ID and then it got some universal acceptance, then, in fact, Crazy Jimmy would not be able to get his password, right?

Ms. CURTIN. That is correct.

Mr. BASS. You can prosecute under Michigan law, and this is technically within the jurisdiction of this subcommittee, but are

there any Federal initiatives that you think ought to be undertaken in the area of criminal justice?

Mr. UPTON. And as you answer that question, you 34 year old that you are going to proceed with charges from last week, I think you indicated that assuming that he is convicted, he is eligible for up to 35 years.

Katie's story, interstate, I mean, all of these different things, 18 months. I mean, did the laws change? Did they just have bad prosecutors? What is the deal?

Mr. GREGART. Well, Michigan's law is rather new. It provides 20 years for using the Internet to commit a felony, and that can be consecutive to the underlying felony, which in our case would be 15 years. So you get in Michigan what is called stat time or consecutive. In other words, you do the 15, and then it is up to the judge's discretion to put 20 on top of that.

That is pretty severe, and I support it.

Ms. TARBOX. In my case he was sentenced in 1998. So there were no precedents about other sentencings. It was a Federal law, and part of the problem is, as I have spoken to other district attorneys or U.S. attorneys, in Frank's case, he was a very wealthy, put together man, and if you meet him, if he came in here, he is very charismatic, and a lot of judges look at these people and think he cannot be that bad, and they have given rather light sentencing, especially because there is a stereotype to what they think pedophiles should be.

I am not a law expert, but you know, from what I have spoken to and other sentencings that I have seen, I mean, somebody got a longer sentencing for not returning library books in Florida than, you know, Frank did for what he has done.

So it is a little crazy, and I think the answer is not, you know—Frank could have been sentenced up to 20 years. The judge did not choose to do so. It is not the legislation's fault. It is the judge's fault.

So we need to communicate that this is really a serious crime, and I Do not think that we have made that step. We need to let people know how detrimental it is.

I know victims of sexual assaults who have had this happen, you know, 5 years ago and are still dealing with it. I feel like I am in a very lucky position. I had parents who could afford the best counseling for me, you know, taking me to the best specialists.

This is not the case for every victim, and so I think a lot of things need to be stepped up, but unfortunately I do not think it is related to this.

Mr. UPTON. Go ahead, Kathy.

Ms. TUCKER. Along the same lines of laws, and so I will direct this to those of you who are currently in law enforcement, when children are first approached on line and you see that contact beginning, such as in the case, and I do apologize. I cannot pronounce your last name.

Mr. GREGART. Me?

Ms. TUCKER. No.

Mr. KARRAKER. Karraker.

Ms. TUCKER. Thank you.

Mr. KARRAKER. John.

Mr. UPTON. John.

Ms. TUCKER. Oh, John? I an deal with that.

In John's case, where he notified, you know, law enforcement that this was going on and there was not anything to be done because there was not a crime, should we not as a Nation look at the total picture and try to put into place some policies that could prevent these acts before they occur rather than always having to deal with after the fact?

Mr. UPTON. And how do these tips ever get passed along to the police authorities when they are able to identify, John?

Mr. KARRAKER. Part of what I was trying to stress with mine, there was no crime that had occurred, but there was the possibility that if law enforcement would have been trained and would have been equipped to deal with it, they could have been notified of the incident. They could have run that case to the point where if he would have committed a crime, that he could have been arrested for it.

And that is the type of education that needs to occur with law enforcement, and also the funding has to be made available to law enforcement.

Mr. UPTON. Ruben?

Mr. RODRIGUEZ. Mr. Chairman, I mentioned that earlier. In John's case, for the law enforcement officer to say there is nothing we can do about it because a crime did not occur, we have heard that all too often. These cases start out somewhere.

Law enforcement officers, if they did not have the resources locally for John or whatever, law enforcement will work these cases. That is how it starts, you know.

Answering your question where did these tips go, when they come to us, we do a lot of validation on the Internet. We have 14 analysts that look at this stuff, peruse the stuff, build probable cause, if you would, to send that information on to law enforcement agencies.

In John's case, I mean, we get these kind of complaints all the time. My child received this. I intercepted that, or whatever.

We give it to law enforcement. They proactively go out there to work undercover operations, assume the child's identity and say, "Okay. I am now 13 year old little Johnny," and you know, start talking. This individual starts sending him child pornography, gets into the grooming process, and you know, he comes to visit her, and he meets this 250 pound burly police officer waiting for him when he gets off of the bus.

So it is being worked. John is perfectly correct. There is a handful of law enforcement officers throughout the United States that work these kind of cases. As I mentioned, the Internet task forces right now, that is 30 independent law enforcement agencies or task forces throughout the country. We need more of those individuals.

We do training for law enforcement out there. The National Center funds these programs to do protecting children on line. AOL is involved in it from the ISP, educating law enforcement officers, how to conduct these investigations.

We have a unit commander course. We bring in the lieutenants and sergeants who work these cases to tell them, you know, these are the issues you are going to have to be dealing with, you know,

the policies, the procedures, or the laws or whatever. And we want to do more and more of those nationwide.

We have standing room only in these courses that we do, but we are not touching as many as we need to talk. I mean, I think the last count was over 800,000 law enforcement officers in the United States. You are talking several hundred individuals who can do these kind of cases.

So there are resources out there. They just have to be expanded.

Mr. UPTON. Well, I want to thank all of you. I want to particularly thank staff. It is never easy, I know, for those of you who came long ways from both ends of the country. Your testimony has been particularly helpful.

This is an issue for not only every state, but certainly every community, every neighborhood, every family, and as we see the great positives of the Internet continue to grow, we have got to be ever so cognizant of some folks wanting to take advantage of a system for their own evil means.

Jim?

Mr. GREGART. Congressman, I think we would be remiss if we only focused on children in this area. Just for all of the adults in the room, I would like to urge you not to respond to the former Nigerian Finance Minister who has E-mailed you asking you for your personal savings and checking account number so that he can transfer $17 million into that account, a classic example, and we have adults across this Nation who are providing their life savings to people they do not know. So you can imagine the problem we have with impressionable children.

Mr. UPTON. That is exactly right.

Okay. I want to thank all of you. It has been terrific, and I just want to say, too, for the press that is here, we will do a little press availability down here for any specific questions you have for the next 15 or 20 minutes. If everyone assembles down here, we will make sure everybody is available for whatever questions you might pose.

Thank you. The hearing is adjourned.

[Whereupon, at 2:57 p.m., the subcommittee was adjourned.]