S. HRG. 110–1103

PROTECTING CHILDREN ON THE INTERNET

HEARING

BEFORE THE

COMMITTEE ON COMMERCE, SCIENCE, AND TRANSPORTATION UNITED STATES SENATE

ONE HUNDRED TENTH CONGRESS

FIRST SESSION

JULY 24, 2007

Printed for the use of the Committee on Commerce, Science, and Transportation

U.S. GOVERNMENT PRINTING OFFICE

72–157 PDF WASHINGTON : 2012

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

SENATE COMMITTEE ON COMMERCE, SCIENCE, AND TRANSPORTATION

ONE HUNDRED TENTH CONGRESS

FIRST SESSION

DANIEL K. INOUYE, Hawaii, *Chairman*

JOHN D. ROCKEFELLER IV, West Virginia	TED STEVENS, Alaska, *Vice Chairman*
JOHN F. KERRY, Massachusetts	JOHN MCCAIN, Arizona
BYRON L. DORGAN, North Dakota	TRENT LOTT, Mississippi
BARBARA BOXER, California	KAY BAILEY HUTCHISON, Texas
BILL NELSON, Florida	OLYMPIA J. SNOWE, Maine
MARIA CANTWELL, Washington	GORDON H. SMITH, Oregon
FRANK R. LAUTENBERG, New Jersey	JOHN ENSIGN, Nevada
MARK PRYOR, Arkansas	JOHN E. SUNUNU, New Hampshire
THOMAS R. CARPER, Delaware	JIM DEMINT, South Carolina
CLAIRE MCCASKILL, Missouri	DAVID VITTER, Louisiana
AMY KLOBUCHAR, Minnesota	JOHN THUNE, South Dakota

MARGARET L. CUMMISKY, *Democratic Staff Director and Chief Counsel*
LILA HARPER HELMS, *Democratic Deputy Staff Director and Policy Director*
CHRISTINE D. KURTH, *Republican Staff Director and General Counsel*
KENNETH R. NAHIGIAN, *Republican Deputy Staff Director and Chief Counsel*

CONTENTS

WITNESSES

PROTECTING CHILDREN ON THE INTERNET

TUESDAY, JULY 24, 2007

U.S. SENATE,
COMMITTEE ON COMMERCE, SCIENCE, AND TRANSPORTATION,
Washington, DC.

The Committee met, pursuant to notice, at 10:06 a.m. in room SR–253, Russell Senate Office Building, Hon. Daniel K. Inouye, Chairman of the Committee, presiding.

OPENING STATEMENT OF HON. DANIEL K. INOUYE, U.S. SENATOR FROM HAWAII

The CHAIRMAN. Without question, the Internet provides extraordinary benefits to our Nation's children. In our schools, teachers use the Internet and computer technology to enhance instruction and enrich student learning. At home, children can use the Internet to exchange e-mail or share pictures with friends and family, and to get information on virtually any subject imaginable.

But the power of the Internet is also a source of its peril. *The New Yorker* once humorously poked fun at the anonymity of the Internet, commenting that, "On the Internet, nobody knows you're a dog." However, there is nothing funny when that same anonymity can be used to the advantage of online predators and others who would seek to harm children.

In addition to protecting their children from online predators, parents also struggle with the challenges of shielding their children from the significant amounts of material on the Internet that aren't suitable for children. While filtering and monitoring technologies help parents to screen out offensive content and to monitor their children's online activities, the use of these technologies is far from universal and may not be foolproof in keeping kids away from adult material. In that context, we must evaluate our current efforts to combat child pornography and consider what further measures may be needed to stop the spread of such illegal material over high-speed broadband connections.

These are all difficult, yet critically important, issues that parents and children face in an information age. If we search for a "silver bullet," we will not find it.

And I will have the rest of my statement made part of the record.

[The prepared statement of Senator Inouye follows:]

PREPARED STATEMENT OF HON. DANIEL K. INOUYE, U.S. SENATOR FROM HAWAII

Without question, the Internet provides extraordinary benefits to our Nation's children. In our schools, teachers use the Internet and computer technology to enhance instruction and enrich student learning. At home, children can use the Inter-

net to exchange email or share pictures with friends and family, and to get information on virtually any subject imaginable.

But the power of the Internet is also a source of its peril. *The New Yorker* once humorously poked fun at the anonymity of the Internet, commenting that, "On the Internet, nobody knows you're a dog." However, there is nothing funny when that same anonymity can be used to the advantage of online predators and others who would seek to harm children.

In addition to protecting their children from online predators, parents also struggle with the challenges of shielding their children from the significant amounts of material on the Internet that are unsuitable for children.

While filtering and monitoring technologies help parents to screen out offensive content and to monitor their child's online activities, the use of these technologies is far from universal and may not be fool-proof in keeping kids away from adult material.

In that context, we must evaluate our current efforts to combat child pornography and consider what further measures may be needed to stop the spread of such illegal material over high-speed broadband connections.

These are all difficult, yet critically important issues that parents and children face in an information age. If we search for a "silver bullet" solution, we will not find it.

Rather, our efforts must rely on a multi-layered strategy—one that teaches our children about safe and responsible online behavior; one that encourages industry action to develop tools that will aid parents in their efforts to restrict inappropriate material from their children's access; and one that relies on swift and certain action by law enforcement officials in finding and punishing those who would use the Internet to harm children.

We have a very distinguished panel of witnesses today to aid our review of this subject. I look forward to their testimony.

The CHAIRMAN. May I now recognize the distinguished Senator from Florida, Senator Nelson.

STATEMENT OF HON. BILL NELSON,
U.S. SENATOR FROM FLORIDA

Senator NELSON. Thank you, to my distinguished Chairman.

One of the most insidious, evil things that is happening in America today is how we are hooking kids through the Internet to explicit material and Internet pornography. It is a plague upon this country. And if we don't take some overt steps to change the legality of this activity, we are going to poison and infect the minds of our children that will have results that will last for generations to come.

Over the past couple of years, we've passed a number of laws, such as the PROTECT Act and the Adam Walsh Act, and made it harder for online predators to go after the kids online. But the predators are always a step ahead of us.

We've seen, for example, the activities start to change from Internet chat rooms to social networking sites, and, on those sites, sexual predators are often able to mask their identity and pose as children, themselves, in order to solicit the children to reveal personal information and to provide pictures and so forth.

As we work to address these threats, we've got work to do, but we also need to look at undertaking a comprehensive effort to educate children about the dangers that lurk on the Internet. A few states, Mr. Chairman, like Virginia, have already created comprehensive lesson plans and curricula to teach Internet safety in their schools. And so, I'm working with others on this committee to formulate legislation that would create a pilot program to provide school districts with grants specifically for Internet safety education.

We teach our kids about school bus safety. We teach them about fire safety. We teach them about storm safety. Maybe—one of the most insidious diseases—we ought to teach them about Internet safety.

Thank you, Mr. Chairman.

The CHAIRMAN. I thank you, Senator Nelson.

Now may I recognize the gentleman from West Virginia, Senator Rockefeller.

STATEMENT OF HON. JOHN D. ROCKEFELLER IV, U.S. SENATOR FROM WEST VIRGINIA

Senator ROCKEFELLER. Thank you, Mr. Chairman.

I like the fact that we're having these hearings, and we're having quite a lot of these hearings. And it was very interesting to me, in a hearing we had several weeks ago on a subject, I think, in which you and I agreed on, that not many members of the Commerce Committee agree on. And so, it came down to this—the idea of indecency was not simply—it was not repellent enough to them, or violence was not repellent enough to them, or vulgarity was not repellent enough to them, so that they were unwilling to overlook, at least in some form, the First Amendment. And it's a little bit like if you're attacked, as a country, and you decide that you're in a peaceful mood, so you're not going to raise an army, you're not going to fight back. I don't think that's the American way. And this meeting this morning is very much along the lines of trying to alert people to the fact that, you know, child pornography sites on the Internet are exploding. They have increased 1,500 percent, according to the National Children's Home Report, since 1988, which is quite a long time ago, but that's also a pretty big increase.

Everybody's always talking about responsible parents, and I think parents want to be responsible, and parents try to be responsible, where they can. There are many places where they can't be, simply because of the situation of their work or their day. Nobody seems to want to talk about the responsibility of those who produce all of this, those who pay for the ads that allow all of this to go onto either the air, if we're talking about television, movies, or onto the Internet. In one of the previous hearings, I deliberately showed some very vulgar stuff that came right off of children's-hour television, and they said, "How can you possibly allow that to go out to children at 10:30 in the morning?" Well, of course, it was on C–SPAN, but that didn't make any difference to them. The point was, you couldn't talk about anything which would in any way compromise the right of children to have their minds polluted, and polluted, in fact, in such a way that many of them will be affected by it for the rest of their lives.

So, I think this is a very serious subject. I think it has a lot to do with the future of America. I like what I heard from the good Senator from Florida, Senator Nelson, what he was saying. And I think it's a very unfunny subject that's going to require some rather drastic action which is going to be displeasing to many. I'm quite prepared to displease the cable industry, the movie industry, the networks, and all the rest of them, and the Internet industry. You know, I don't think that's what's at stake here. I think what's at stake is the health and the safety and the disposition of our chil-

dren as they grow older and what it is they carry in their minds, and what habits they develop.

Thank you, Mr. Chairman.

The CHAIRMAN. I thank you very much.

Before we proceed, I should advise you that I've just received a note from the leadership that votes will commence at 10:30. So, I may have to call a recess at some later time.

This morning, we have a very distinguished and lovely panel. We have the lovely Lauren Nelson, Miss America of 2007; Mr. David Finkelhor, Director of Crimes Against Children Research Center of the University of New Hampshire; Mr. Ernie Allen, President and Chief Executive Officer, National Center for Missing & Exploited Children; Mr. Lan W. Neugent, Assistant Superintendent for Technology and Human Resources, Virginia Department of Education; and Ms. Christine N. Jones, General Counsel and Corporate Secretary, The Go Daddy Group, Incorporated.

And it's my privilege and pleasure to call upon the lovely Miss America of 2007, Miss Nelson.

STATEMENT OF LAUREN NELSON, MISS AMERICA 2007

Ms. NELSON. Thank you very much, Senator.

As Miss America, I have the opportunity to travel around and champion a cause that is very, very important to me. I travel about 20,000 miles a month, speaking on the issue of Internet safety, because I had a personal incident with the issue of Internet Safety.

As a 13-year-old girl, I was having a sleepover with two of my girlfriends, and we decided that we would get into a chat room. We were talking with people that we did know and people that we didn't know, which was our first mistake. And the conversations continued. We were approached by a man who was older than us, and he asked us the question, "ASL," which means, "Age, Sex, Location." And we gave him the information, willingly, not knowing any better. So, within an instant, he knew that we were girls, he knew were females, and he knew where we were in Oklahoma, which is ultimately enough information for him to track us down. Luckily, that did not happen, but, about a week later, he sent inappropriate pictures of himself, and then we alerted our parents, and they alerted the proper authorities.

These stories happen all the time, and most kids are not as lucky as I was and as my friends were. Seventeen million children between the ages of 13 and 17 are online, and one in five of those children are approached every day by an online predator. As you said, social networking sites and chat rooms and instant messaging are huge on the Internet, and it's huge for our kids. Seventy-one percent of kids have a social networking site; 64 percent of those kids actually post pictures and videos of themselves on those sites; and over half of them leave information on the Internet about where they're located and where they live. And this is part of the problem.

As I said, through my travels I've had the opportunities to meet with Ernie Allen, at the National Center for Missing & Exploited Children, and I've also been introduced to John Walsh, who is also a huge champion of this issue. After my introduction to John Walsh, I had the opportunity to work with the America's Most

Wanted television show and do a sting operation. And, as my participation in the sting operation, I ultimately was the 14-year-old decoy at the sting house. I chatted online with these men, I talked on the phone with them and was the 14-year-old girl that met them at the door that they followed into the house. So, I've gotten to see, from all points of view, how this issue affects kids and how it affects these people that are involved with it.

Through my participation with that operation, I learned a little bit more about how predators behave. They prey on the most vulnerable of our children, the kids that are having problems at home. Maybe they don't have friends at school. But these kids divulge this information, and these predators know that, and they use emotional tactics to get in there and to make sure that they lay the groundwork to make them comfortable with themselves so that they can get more information with them and ultimately meet them in person.

I've also had the opportunity to work with Cox Communications, and, just last month, had the opportunity to be at the Teen Summit, where we had 14 kids from 14 different States across the U.S. come and tell us a little bit about their Internet habits, what they were worried about, and what they wanted us to do, as adults. And one of the neatest things that we found that day was that the kids actually want parents to be involved with what they're doing on the Internet, they want their parents to ask questions, but they want their parents to know how to ask the questions, and not to make it an interrogation.

We also learned that cyber-bullying is a huge problem. Not only do we have to worry about, now, predators, but we also have to worry about kids and how they're using the Internet. There was a story that I recently read, that a child was being cyber-bullied, and he actually committed suicide because of it, and his parents had no idea what was going on. Cyber-bullying is a rampant problem on the Internet.

So, I'm here today to urge you to implement mandatory education for our children about Internet safety. I know that computer classes are in high schools, are in even middle schools, and they're learning ways to use the computer. Why not implement some Internet education so that they know the dangers, also the opportunities, of the Internet, but also learn how to be courteous cyber citizens. We don't allow our children to cross the street without knowing how to do it. We don't allow our children to drive a car without giving them proper education. We shouldn't allow them to go on the Internet without knowing the dangers and the opportunities at the same time.

I feel that it's the responsibility of kids, of parents, of schools, and of government officials to make a change in this problem.

So, thank you for having me here.

[The prepared statement of Ms. Nelson follows:]

PREPARED STATEMENT OF LAUREN NELSON, MISS AMERICA 2007

My name is Lauren Nelson and as Miss America 2007, I am proud to be here today to discuss the issue of Protecting Children on the Internet. This is a subject that has personally touched my life. When I was 13 years old, my friends and I were approached on the Internet through a chat room. We were young and did not know of the dangers of the internet, so we provided this person with our names, ages, gen-

der, and our home addresses. A few days later, the individual sent us inappropriate photos. We were shocked and disgusted. We then told our parents, who immediately addressed this incident and reported it to the proper authorities, and luckily we were able to avoid a potentially dangerous situation.

Not all children are as lucky as my friends and I were.

As Miss America 2007, I have made this issue my personal platform and I am here today to champion this cause. During my year of service, I am visiting cities across the country, speaking to parents, children and the media about the dangers of the Internet and the ways we can incorporate Internet Safety into our children's lives.

Back in the April, I had the opportunity to meet with the National Center for Missing and Exploited Children who shared with me their knowledge of Internet crimes against children. They introduced me to John Walsh and the television producers for Americas Most Wanted. After meeting with the producers of AMW, my commitment grew even stronger to do something that would bring national attention to this issue and get people talking about ways to stop these horrible crimes against children.

When I heard about the Sting Operation being conducted by the Suffolk County Police Department and America's Most Wanted, I immediately wanted to get involved. My role in the Sting Operation was to pose as a 14-year-old girl. I would visit chat rooms and wait to be approached. It was shocking to me how quickly a benign conversation would turn sexual. The suggestions these men were making coupled with the fact that they thought they were chatting with a 14-year old, turns my stomach to this day. It was incredibly disturbing to me how young teens can so easily be approached on the Internet and ultimately, meet face to face with very dangerous individuals who disguise themselves through the veil of the computer. Eleven predators showed up in person during our Sting Operation . . . and this can not be tolerated in our society.

Upon my last visit to D.C., I had the opportunity to be a part of the Teen Summit on Internet Safety with John Walsh and we were amazed at the teens' responses to the questions regarding their Internet habits. Can you believe that one out of fourteen teens gives out their personal information on the Internet without knowing who they are chatting with?

It is clear that our teens are not adequately educated on the dangers that the Internet can pose or the consequences they may face by sharing personal information with strangers. That is the reason I am here today.

I believe it is time to government to get involved and provide mandatory education for all of our children. We need to begin educating children as early as possible. We have all heard someone say "My kids/grandkids are quicker on the computer then I am." It's so true. Kids today are growing up using computers from a very early age and using them on a daily basis. We don't allow our children to ride their bikes without first teaching them about proper safety and we shouldn't let them use the computer and access the Internet without taking the same precautions.

I am here today to ask you to please implement mandatory education on Internet Safety for all of our children. There should be a mandatory class on Internet safety that teaches children about how to use the internet, the potential dangers of the internet, and how to avoid these dangers.

As students become more proficient on the computer, they should be taught about the various networking sites and chat rooms, and the problems that can occur when they mis-use these sites.

Lastly, they should also learn about being responsible cyber citizens. The issue of cyber-bullying is a growing problem in our schools today and it must be addressed now. The bullies have moved from the playgrounds to the internet, and this new form of harassment cannot be tolerated.

Through proper education, awareness and a national effort supported by our legislators, we can all begin to make a difference. I sincerely hope that by using my voice as Miss America to bring awareness to this subject, that the message of the importance of Internet Safety education for our children will be heard. Thank you.

The CHAIRMAN. Ms. Nelson, I've been in the Government for many years, and, during that period, I've heard over 1,000 witnesses, and, without question, your testimony is one of the most informative and articulate. I thank you very much.

Ms. NELSON. Thank you.

The CHAIRMAN. Our next witness is Dr. David Finkelhor.

STATEMENT OF HON. TED STEVENS, U.S. SENATOR FROM ALASKA

Senator STEVENS. Mr. Chairman, would you allow me to put my statement in the record, just——

The CHAIRMAN. Without objection.

Senator STEVENS.—as though read? Thank you.

[The prepared statement of Senator Stevens follows:]

PREPARED STATEMENT OF HON. TED STEVENS, U.S. SENATOR FROM ALASKA

The Internet is a dynamic space where Americans turn to get information, do research, and exchange ideas.

Given the increasingly important role of the Internet in education and commerce, it differs from other media like TV and cable because parents cannot prevent their children from using the Internet altogether. The headlines continue to tell us of children who are victimized online. While the issues are difficult, I believe Congress has an important role to play to ensure that the protections available in other parts of our society find their way to the Internet. Since introducing the Protecting Children Online in the 21st Century Act, my staff and I have worked with a wide variety of advocacy groups on this topic. In response to the feedback we have received, my staff are currently circulating a new draft with four primary goals.

The new measure would:

- direct the Federal Communications Commission to identify industry practices that can limit the transmission of child pornography;
- require schools that receive E-Rate funds to provide age-appropriate education to their students regarding online behavior, social networking and cyber-bullying;
- require the Federal Trade Commission to form a working group to identify blocking and filtering technologies in use and identify, what, if anything could be done to improve the process and better enable parents to proactively protect their children online; and
- add the selling or purchasing of children's personal information in connection with a criminal offense in the criminal code as an indictable offense.

I hope the panelists can give us more insight on what we can do within the First Amendment to empower parents and whether this bill heads in the right direction.

The CHAIRMAN. Please proceed. Dr. Finkelhor?

STATEMENT OF DR. DAVID FINKELHOR, DIRECTOR, CRIMES AGAINST CHILDREN RESEARCH CENTER, HORTON SOCIAL SCIENCES CENTER, UNIVERSITY OF NEW HAMPSHIRE

Dr. FINKELHOR. Yes, thank you very much. Appreciate the invitation to be here and your interest in this very important issue.

I'm the director of the Crimes Against Children Research Center at the University of New Hampshire.

Whenever new threats appear on the scene, like SARS or schoolshooters, it's really crucial to characterize them accurately and as soon as possible, because first impressions are lasting impressions, and it's often hard to change these impressions later on. We need accurate and early characterizations to get people focused on the right thing to prevent the spread of these dangers.

Now, in the case of Internet safety, though, I'm afraid that we may be off to a poor start on some issues. I think the public impression of this crime is really not in sync yet with the reality, based on what we know from the research. And it's this reality that I think needs to guide our public education as we get around to doing it.

The public image of this crime is that we have Internet pedophiles, who have moved from the playgrounds into your living room through your Internet service, who are targeting young children by pretending to be other children, who are lying about their ages, identities, and motives, who are tricking kids into providing personal information like their names and their addresses, or who harvest these things from MySpace, and then, armed with this information, these criminals stalk children, abduct them, rape them, or worse.

But, actually, the research suggests a somewhat different reality. And here's what we've found now, based on hundreds of cases that we've reviewed from national surveys of law enforcement agencies and two large national studies of youth Internet users themselves. Incidentally, all this research is available in prominent medical and scientific journals. I can make them available to you, if you'd like.

First we found that the predominant online sex crime victims are not young children, they are teenagers. And the predominant crime scenario does not involve violent stranger molesters posing online as other children in order to set up an abduction or an assault. It turns out only about 5 percent of the online sex crimes against children involve violence when meetings occur, and only 3 percent entail an abduction. And, interestingly, deception is not a major factor, either. Only 5 percent of the offenders truly concealed the fact that they were adults from their victims, and 80 percent, by contrast, were quite explicit about their sexual intentions toward the kids in their interactions with them somewhere along the line.

So, these are not primarily violent sex crimes, but, rather, I would characterize them as criminal seductions that take advantage of common teenage vulnerabilities. The offenders lure teens to meet them for sexual encounters after weeks of, very often, quite explicit online conversations that play on the teen's desire for romance, adventure, sexual information, and understanding. And, as Lauren said, these are often troubled youth with histories of family turmoil and physical and sexual abuse, as well.

So, to take a representative case, Jenna, a 13-year-old girl from a divorced family, she frequently went to sex-oriented chat rooms, under the screen name "evil—girl." There, she meets a 45-year-old guy, Dave. He flatters her, gives her gifts, talks to her about intimate things, and then drives across several State lines to meet her for sex; on several occasions, in motel rooms. Dave is arrested with her in one of these rooms. Jenna resists cooperating with the police.

And many of the Internet sex crimes have commonalities with this case. In 73 percent of the crimes, the youth go to meet the offender on multiple occasions, for multiple sexual encounters. Half the victims were described by the police investigators as "being in love" or "feeling close friendship" with the offender. In a quarter of the cases, the victims actually ran away from home to be with the offender.

And I think these are aspects of Internet crimes against youth that haven't been fully incorporated into our thinking yet, and they have lots of implications for prevention. So, for one thing, we think it means that we have to make sure our messages are directed at

teens, teens themselves, in language, in format, and from sources that they relate to. We've directed a lot of our information, up until now, at parents; but, many of these teens are under limited parental influence.

We also have to get beyond blanket warnings about not giving out personal information. Our research, in fact, has suggested that giving out personal information is not what puts kids at risk, neither does having a blog or a personal website or a MySpace social networking site. What puts kids in danger for these crimes is being willing to talk online about sex, with strangers, having multiple risky activities on the Web, like going to these chat rooms or sex sites, or interacting with a lot of people online whom they don't know. It's the kids who move toward, rather than away from, the first signs of danger that I think we need to be thinking about.

So, in order to prevent these crimes, we have to broach more awkward and complicated topics that start with an acceptance of the fact that some teens are curious about sex. They are looking for romance and adventure online. We need to talk with them frankly about some of the risky things that they may be contemplating; why hooking up with a 32-year-old guy has major drawbacks, like jail or bad publicity or public embarrassment; why they should be discouraging, not patronizing, sites and people who are doing offensive and weird things online, fascinating as these things might seem to them.

We also need to do things like making it easier for teens to report the come-ons and the sexual picture requests. We need to empower bystanders to take action. There are often friends or online observers in chat rooms who may see what's happening, but who today aren't doing anything to stop it.

We could also do things like task some of our Federal agencies, like the CDC, OJJDP, organizations like the NCMEC, to help design scientifically grounded prevention programs that address these issues and that can be disseminated to educate youth based on proven effectiveness. And this is important. I don't think we should be just telling people to do prevention without providing solid guidelines about what really works. And, unfortunately, I'm not sure that we know, yet, exactly what works.

We also need law enforcement training, so that they know how to handle these cases, and how to deal with the fact that the kids in these cases are often reluctant, as witnesses, and make prosecution difficult. They need to know how to work with them to bring them along.

We need training for school officials, mental health professionals. These are the kind of people who have contact with some of these at-risk youth before they get into trouble.

And then, we need ongoing research just to keep tabs on what kids are experiencing and also what law enforcement is encountering, because one of the things about the Internet environment is that it is a very rapidly changing one, and the threats and dangers can morph very quickly, and we have to stay on top of these changes. We don't want to be responding to yesterday's problems. We don't, also, want to be overgeneralizing from a single high-profile incident.

For example, I think we could use an annual assessment of threats to kids in the Internet environment, something like the annual Monitoring the Future, national survey about drug usage, that gives us clues about new trends in drug usage that may be plaguing the youth population.

But the prevention challenges here aren't easy. Like discouraging kids from smoking or drinking, simple scare tactics really don't work. The challenge requires some really very deft maneuvering within the teen psychology, which is often obscure, to figure out what will stick there. And, in the meantime, we have to be cautious about promoting messages that may simply turn teens off or that betray a completely unrealistic take on the Internet, and that may make them less receptive to the authoritative sources that we really want them ultimately to trust on this issue. I don't think we should allow a sense of crisis to mobilize us into misguided crusades.

So, I'm saying we have to do our homework, we have to do our research. So much happens online that's hidden. But if we want to stop these Internet crimes, we have to understand the details of what's going on. It's as simple and as complicated as that.

Thank you.

[The prepared statement of Dr. Finkelhor follows:]

PREPARED STATEMENT OF DR. DAVID FINKELHOR, DIRECTOR, CRIMES AGAINST CHILDREN RESEARCH CENTER, UNIVERSITY OF NEW HAMPSHIRE

Whenever any new threats appear on the scene, from SARS to school shooters, it is so crucial to characterize them accurately and as soon as possible, because first impressions are lasting impressions, and it is hard to change them later. We need such accurate and early characterizations to get people to be focused on the right things to do to prevent the spread of the danger.

Now in the case of Internet sex crimes against children, I'm afraid we may already be off to a poor start. The public impression of this crime is not in sync with the reality of this crime based on what we now know from the research, the reality that I think needs to guide our public education.

The public impression about this crime is that we have "Internet pedophiles", who have moved from the playgrounds into your living room through your Internet service, who target *young* children by pretending to be other children, who lie about their ages, identities and motives, who trick the children into providing personal information like their names and addresses, or who harvest it from MySpace; and then armed with this information, these criminals stalk the children, abduct them, rape them or worse.

But our research suggests a different reality. Here's what we have found based on hundreds of cases retrieved from national surveys of law enforcement agencies, and two large national interview studies of youth Internet users themselves, all this research is available now in articles in prominent medical and scientific journals.

First, we have found that the predominant online sex crime victims are not young children, but rather teenagers. And the predominant crime scenario does not involve violent stranger molesters posing online as other children in order to set up an abduction and an assault. Only 5 percent of the online sex crimes against children involved violence when meetings occurred, only 3 percent entailed an abduction.

Nor is deception a major factor. Only 5 percent of offenders truly concealed the fact that they were adults from their victims and 80 percent by contrast were quite explicit about their sexual intentions toward these kids in their interactions with them.

These are not mostly violent sex crimes but rather criminal seductions that take advantage of common teenage vulnerabilities. The offenders lure teens to meet them for sexual encounters after weeks of very often quite explicit online conversations that play on the teen's desires for romance and adventure and sexual information and understanding. These teens are often troubled youth with histories of family turmoil and physical and sexual abuse as well.

Jenna was a computer-savvy 13 year old, from a divorced family who frequented sex-oriented chat rooms under the screen name "evil—girl." There she meets a 45 year old, Dave. He flatters her, gives her gifts, jewelry, talks about intimate things and drives across several states to meet her for sex on several occasions in motel rooms. When Dave is arrested with her, Jenna resists cooperating with police.

Many of the Internet sex crimes have commonalities with this case. In 73 percent of these crimes, the youth go to meet the offender on multiple occasions, for multiple sexual encounters. Half the victims were described by police investigators as being in love with or feeling close friendship with the offender. In a quarter of the cases the victim actually ran away from home to be with the offender. These are aspects of Internet crimes against youth that haven't been fully incorporated into our thinking.

They have lots of implications for prevention. For one thing, we think it means that we need to make sure our messages are directed at teens, in language and format and from sources they relate to. Teens themselves, not primarily parents. Many of these teens may be under limited parental influence.

We also have to go beyond blanket warnings about not giving out personal information. Our research with youth suggests that giving out personal information is not what puts kids at risk. Nor does having a blog or a personal website or frequenting My Space. What puts kids in danger for these crimes is being willing to talk about sex online with strangers, and having a pattern of multiple risky activities on the web—like going to sex sites and chat rooms, and interacting with lots of people there. It's kids who move toward rather than away from the first signs of danger.

So to prevent these crimes, we have to take on more awkward and complicated topics and start with an acceptance of the fact that some teens are curious about sex and looking for romance and adventure online: We need to talk to them frankly about the risky things they might be contemplating—about why hooking up with a 32 year old has major drawbacks, you know, like jail, bad press, public embarrassment ; and why they should be discouraging, not patronizing, sites and people who are doing offensive things online, fascinating as they may seem.

We also need to make it easier for teens to report the come-ons and the sexual picture requests, and we need to empower by-standers to take action—that is, the friends and the online observers in chat rooms, who may see this happening but today do little to stop it.

We need to task agencies that know about prevention, like CDC and OJJDP and NCMEC, to help design scientifically grounded prevention programs that address these issues and that can then be disseminated to educate youth based on their proven effectiveness. We shouldn't just tell people to do prevention without providing solid guidelines about what really works. And unfortunately, I am not sure we that we know yet what really works.

We need training for law enforcement, so they know how to handle these cases and the often reluctant kids whom they need as witnesses to prosecute the offenders.

We also need training for school officials and mental health professionals, so they, too, can help some of these at risk kids before they get into trouble.

And then we need ongoing research to keep tabs on what kids are experiencing and what law enforcement is encountering, because in this rapidly changing technological environment the threats and dangers can morph so very quickly. We have to stay on top of them. We don't want to be responding to yesterday's problem. We don't want to be over-generalizing from one single, high profile incident. So for example, I think we need an annual assessment of threats to kids in the Internet environment, something like the annual Monitoring the Future national survey about drug usage.

The prevention challenges here are not easy. Like discouraging kids from smoking or drinking, the simple scare tactics often don't work. This challenge too may require very deft maneuvering within the teenage psychology to get the message to stick. And in the meantime, we need to be cautious about promoting messages that turn teens off or that betray a completely unrealistic take on the Internet and which may only make them less receptive to the authoritative sources that we want them ultimately to trust on these issues. We shouldn't allow a sense of crisis to mobilize us into misguided crusades.

So we have to do our homework. We have to do our research. So much of what happens online is so hidden. But if we want to stop these Internet crimes, we have to understand the details of what is going on. It is as simple and as complicated as that.

The CHAIRMAN. I thank you very much.

May I now call upon Mr. Ernie Allen.

STATEMENT OF ERNIE ALLEN, PRESIDENT AND CEO, NATIONAL CENTER FOR MISSING & EXPLOITED CHILDREN

Mr. ALLEN. Thank you, Mr. Chairman.

Mr. Chairman, let me first express my gratitude to this Committee, which I know has examined this issue and discussed this issue for some time. I was honored to appear before this Committee last fall in a similar hearing that resulted in a number of initiatives, including Senator McCain and Senator Schumer's SAFE Act legislation, which we think provides a major step forward. So, we're delighted to be here with you again.

What I would like to do is talk briefly about what we have learned, at the National Center for Missing & Exploited Children, about this problem.

Since 1998, with the mandate of Congress, we have operated the CyberTipline, the 911 for the Internet, handling reports from the public and from Internet service providers regarding child sexual exploitation online. Two weeks ago, we handled our 500,000th report. And what we have learned is that this is a huge and evolving challenge for law enforcement, for the public, and for communities.

The challenges include technology challenges. For example, last year, working with six major Internet companies, we created a technology coalition in an effort to develop new technology to identify illegal images online, and interdict them, including creating a database of known images so that we can prevent their reaching consumers.

Another challenge is the growth of digital photography, Web cams and the ease of creating images. Dr. Finkelhor talked about the fact—and, in his research, demonstrates—that, increasingly, many of these images are self-created. Kids are taking photos and distributing themselves, having either been seduced or at least insufficiently sensitive to the risks which they're posing.

In 1982, the Supreme Court of the United States said that child pornography is not protected speech; it's child abuse. And, as a result, through law enforcement efforts, it largely disappeared from the shelves of adult bookstores and through the mail. What we now know is that it went underground, and, when it went underground, with the advent of the Internet, it exploded. I talk frequently about one case, generated from a lead we received at the CyberTipline, that led us to husband-and-wife entrepreneurs who decided to go into the child pornography business. When the site was shut down and they were arrested, these people had 70,000 customers, paying $29.95 a month and using their credit cards to access graphic images of small children being raped and sexually assaulted.

New technology has enabled child pornographers to stay a step ahead of law enforcement. For example, many distributors of child pornography are now using peer-to-peer file-sharing networks, which do not use a central server, depriving law enforcement of an identifiable Internet Protocol, or IP, address.

Wireless technology, with the increase in connectivity enabling people to access the Internet through wireless devices, has increased the size of this problem.

In 1998, this Congress mandated electronic service providers to report child pornography on their systems to law enforcement via the National Center for Missing & Exploited Children. The good news is that today 327 electronic service providers are regularly reporting. The bad new is, thousands more aren't. We have worked with the U.S. Internet Service Providers Association, developing best practices regarding guidelines to address this problem. The major ISPs are reporting, but our concern is that safe havens are being created in nonparticipating ISPs, and we need to do more about it.

The U.S. Department of Justice has indicated that the underlying statute is flawed, and this is one of the issues we discussed with this Committee last year. We need to fix that statute so that every ISP is required to report.

There is another missing link. Currently, the statute constrains the National Center, in that we are only able to forward those leads to U.S. law enforcement. One major ISP tells us, for example, that much of its system is used in Brazil. That provider wants to send us information about child pornography they find on their customers' accounts to Brazilian law enforcement. We're precluded from doing that.

There is another missing link that we've discussed in the past. Once our CyberTipline analysts, who look at these images, triage them, use search tools and techniques to try to identify who the sender, who the distributor is, and then provide them to the appropriate law enforcement agency—once they've done that, there can be no prosecution until the date and time of that online activity is connected to an actual person. And there is currently no requirement for providers to retain connectivity logs for their customers on an ongoing basis. Some have policies on retention, many of them excellent. But they vary, are not implemented consistently, and are far too short a time to have meaningful prosecutorial value.

We've taken some new initiatives. In the area of commercial child pornography, through the leadership of Senator Shelby, who was then the chairman of the Senate Banking Committee, in the Banking Committee, we've created a financial coalition against child pornography that includes 29 major companies, including MasterCard, Visa, American Express, Bank of America, Citibank, Google, Yahoo!, AOL, Microsoft. The goal is to follow the money. These are illegal transactions and an illegal use of the payment system. Law enforcement gets first crack, but law enforcement can't possibly arrest and prosecute everybody, so we're trying to use existing law, existing banking law, to stop the payments, shut down the accounts, and put these people out of business. The goal is to increase the risk and eliminate the profitability.

Mr. Chairman, I don't come before you today with a quick, easy solution to the problem, but I can state unequivocally that the advent of the Internet has provided predators with means to entice children into sexual acts, and sustain—and create—a new lucrative illegal commercial enterprise based on victimizing children. Federal, State, and local law enforcement are more aggressive in this effort than ever before. There is a new Justice Department initiative, called Project Safe Childhood, which is attacking this problem. But they face significant barriers. I hope that you, in this Com-

mittee, can help us remove some of those barriers and help us identify and prosecute more of the individuals who are preying upon children online.

[The prepared statement of Mr. Allen follows:]

PREPARED STATEMENT OF ERNIE ALLEN, PRESIDENT AND CEO, THE NATIONAL CENTER FOR MISSING & EXPLOITED CHILDREN

Mr. Chairman and distinguished Members of the Committee, as President of the National Center for Missing & Exploited Children (NCMEC), I welcome this opportunity to appear before you to discuss crimes against children on the Internet. NCMEC joins you in your concern for the safety of the most vulnerable members of our society and thanks you for bringing attention to this serious problem facing America's communities.

Let me first provide you with some background information. NCMEC is a not-for-profit corporation, mandated by Congress and working in partnership with the U.S. Department of Justice as the national resource center and clearinghouse on missing and exploited children. NCMEC is a true public-private partnership, funded in part by Congress and in part by the private sector. Our Federal funding supports specific operational functions mandated by Congress, including a national 24-hour toll-free hotline; a distribution system for missing-child photos; a system of case management and technical assistance to law enforcement and families; training programs for Federal, state and local law enforcement; and programs designed to help stop the sexual exploitation of children.

These programs include the CyberTipline, the "9–1–1 for the Internet," which serves as the national clearinghouse for investigative leads and tips regarding crimes against children on the Internet. The Internet has become a primary tool to victimize children today, due to its widespread use and the relative anonymity that it offers child predators. Our CyberTipline is operated in partnership with the Federal Bureau of Investigation ("FBI"), the Department of Homeland Security's Bureau of Immigration and Customs Enforcement ("ICE"), the U.S. Postal Inspection Service, the U.S. Secret Service, the U.S. Department of Justice's Child Exploitation and Obscenity Section and the Internet Crimes Against Children Task Forces, as well as state and local law enforcement. Leads are received in seven categories of crimes:

- possession, manufacture and distribution of child pornography;
- online enticement of children for sexual acts;
- child prostitution;
- child-sex tourism;
- child sexual molestation (not in the family);
- unsolicited obscene material sent to a child; and
- misleading domain names.

These leads are reviewed by NCMEC analysts, who visit the reported sites, examine and evaluate the content, use search tools to try to identify perpetrators, and provide all lead information to the appropriate law enforcement agency. The FBI, ICE and Postal Inspection Service have "real time" access to the leads, and all three agencies assign agents and analysts to work directly out of NCMEC and review the reports. The results: in the 9 years since the CyberTipline began operation, NCMEC has received and processed more than 500,000 leads, resulting in hundreds of arrests and successful prosecutions.

However, despite this progress the use of the Internet to victimize children continues to present challenges that require constant reassessment of our tools and methods. As technology evolves, so does the creativity of the predator. New innovations such as webcams and social networking sites are increasing the vulnerability of our children when they use the Internet. New technology to access the Internet is used by those who profit from the predominantly online market in child pornography and seek to evade detection by law enforcement.

Today, NCMEC is working with leaders in many industries involved with the Internet in order to explore improvements, new approaches and better ways to attack the problems. We are also bringing together key business, law enforcement, child advocacy, governmental and other interests and leaders to explore ways to more effectively address these new issues and challenges.

Last year, six Internet industry leaders, AOL, Yahoo, Google, Microsoft, Earthlink and United Online, initiated a Technology Coalition to work with us to develop and

deploy technology solutions that disrupt the ability of predators to use the Internet to exploit children or traffic in child pornography. The Technology Coalition has four principal objectives:

1. Developing and implementing technology solutions;
2. Improving knowledge sharing among industry;
3. Improving law enforcement tools; and
4. Researching perpetrators' technologies to enhance industry efforts.

Bringing together the collective experience, knowledge and expertise of the members of this Coalition, and applying it to the problem of child sexual exploitation, is a significant step toward a safer world for our children.

In June 2006, NCMEC hosted a Dialogue on Social Networking Sites here in Washington, D.C. We did this to respond to the increased attention to these hugely popular sites that permit users to create online profiles containing detailed and highly personal information, which can be used by child predators to forge a "cyber-relationship" that can lead to a child being victimized. This vigorous and informative discussion brought together leaders from the technology industry, policymakers, law enforcement, academia and children's advocacy groups. We learned a lot about why children are drawn to these sites, the technological capabilities and limitations of the site operators who are concerned about the safety of their users, and how law enforcement sees these sites as both a danger to kids and a useful source of information in investigating cases. NCMEC is continuing to work with several social networking sites on ways to make children less vulnerable.

Another challenge is the widespread use of the webcam, which offers the exciting ability to see the person you're communicating with over the Internet. While this has many benefits, such as allowing divorced parents to have "online visitation" with their children in distant states, it, too, can be used to exploit children. The reports to our CyberTipline include incidents involving children and webcams. Many children are victimized inadvertently, by appearing on their webcams without clothes as a joke, or on a dare from friends, unaware that these images may end up in a global commercial child pornography enterprise. Other children are victims of blackmail, threatened with disclosure to friends and family if his or her 'performance' before the webcam doesn't become more sexually explicit. Too much technology and too much privacy, at a sexually curious age, can lead to disastrous consequences.

But the most under-recognized aspect of the Internet is how it is used to distribute child pornography. It is not an exaggeration to state that this is a crisis of global proportions.

Following the Supreme Court's 1982 decision in *Ferber* v. *New York,* holding that child pornography was not protected speech, child pornography disappeared from the shelves of adult bookstores. The U.S. Customs Service launched an aggressive effort to intercept it as it entered the country and the U.S. Postal Inspection Service cracked down on its distribution through the mails. However, child pornography did not disappear, it went underground.

That lasted until the advent of the Internet, when those for whom child pornography was a way of life suddenly had a vehicle for networking, trading and communicating with like-minded individuals with virtual anonymity and little concern about apprehension. They could trade images and even abuse children "live," while others watched via the Internet.

Then law enforcement began to catch up, and enforcement action came to the Internet. The FBI created its Innocent Images Task Force. The Customs Service expanded its activities through its Cyber Crimes Center. The Postal Inspection Service continued and enhanced its strong attack on child pornography. Congress created and funded the Internet Crimes Against Children (ICAC) Task Forces at the state and local levels across the country. There are currently forty-six ICAC Task Forces and the Adam Walsh Act, enacted 1 year ago, will create ten more. Child pornography prosecutions and convictions have increased.

But we should have no illusions about the impact of these initiatives on what has become a financially lucrative industry.

The Internet has revolutionized the commercial markets for virtually every type of goods and services that can be sold. Unfortunately, this also includes goods and services that subsist on the victimization of children. In a recent case investigators identified 70,000 customers paying $29.95 per month by credit card for Internet access to graphic images of small children being sexually assaulted. In our experience, most of the consumers are here in the U.S., and we have found that of the 820 identified victims in NCMEC's Child Victim Identification Program, a startling number of these children are also here in the U.S.

A recent report by McKinsey Worldwide estimated that today commercial child pornography is a multi-billion-dollar industry worldwide, fueled by the Internet. There is also strong evidence of increasing involvement by organized crime and extremist groups. Its victims are becoming younger. According to NCMEC data, 19 percent of identified offenders had images of children younger than 3 years old; 39 percent had images of children younger than 6 years old; and 83 percent had images of children younger than 12 years old. Reports to the CyberTipline include images of brutal sexual assaults of toddlers and even infants. These are images that no one here could previously even imagine. But they have become all-too-common in the new world of child pornography and child sexual exploitation. Children have become, simply put, a commodity in this insidious commercial enterprise.

New technology has allowed this industry to stay one or two steps ahead of law enforcement. Many distributors of child pornography are using peer-to-peer file-sharing networks, which does not use a central server, thereby depriving law enforcement of an identifiable Internet Protocol (IP) address, which is key evidence in investigating and prosecuting these cases. When we receive these reports to the CyberTipline, it is almost impossible to identify the perpetrators responsible for trading the illegal files. The anonymity of recent peer-to-peer technology has allowed individuals who exploit children to trade images and movies featuring the sexual assault of children with very little fear of detection.

Wireless access to the Internet permits predators to "piggyback" on others' wireless signals, trade images, and remain undetected by law enforcement because of the difficulty in locating the piggybacking activity, compounded by the increasing use of wireless access cards manufactured overseas which use radio channels not authorized by the Federal Communications Commission. Wireless technology has also enabled the trading of these images via cell phone—making the operation of this enterprise not only mobile, but also able to fit inside a pocket and easily discarded to avoid detection.

Another obstacle to overcome is the reporting of child pornography found on customers' accounts by electronic service providers (ESPs) to NCMEC. Though apparently mandated by Federal statute, 42 U.S.C. § 13032, not all ESPs are reporting and those that do report are not sending uniform types of information, rendering some reports useless. Some ESPs take the position that the statute is not a clear mandate and that it exposes them to possible criminal prosecution for distributing child pornography themselves. In addition, because there are no guidelines for the contents of these reports, some ESPs do not send customer information that would allow NCMEC to identify a law enforcement jurisdiction. As a result, potentially valuable investigative leads are left to sit in the CyberTipline database with no action taken. Together with the U.S. Internet Service Providers Association (USISPA) we developed 'best practices' reporting guidelines to address this problem. The major ESPs are following these guidelines—for example, AOL, Microsoft, and Yahoo. However, these are voluntary rather than mandatory, so there is no enforcement mechanism for those who choose not to follow them.

This reporting statute also constrains NCMEC in that it permits us to forward the CyberTipline leads only to U.S. law enforcement. This is a real problem, considering the global nature of the Internet. As an example, there is a portion of one major ESP system based in the U.S. that is used primarily in Brazil. This ESP wants us to send information about child pornography they find on their customers' accounts to Brazilian law enforcement. But we are prohibited from doing so.

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

We think this is just not acceptable.

One of our new initiatives treats this industry like the business that it is. Our goal: to eradicate commercial child pornography. Our mission: to follow the money. This new initiative is the Financial Coalition Against Child Pornography.

First, we will aggressively seek to identify illegal child pornography sites with method of payment information attached. Then we will work with the credit card industry to identify the merchant bank. Then we will stop the flow of funds to these sites. The Coalition is made up of major financial and Internet companies, including MasterCard, Visa, American Express, Bank of America, Citibank, Microsoft, America Online, Yahoo and many others. We are working to bring new members into the Coalition every day, especially international financial institutions.

The first priority in this initiative is criminal prosecution, through referrals to Federal, state, local or international law enforcement in each case. However, our fundamental premise is that it is impossible to arrest and prosecute everybody. Thus, our goal is twofold:

1. To increase the risk of running a child pornography enterprise; and
2. To eliminate the profitability.

NCMEC is working hand-in-hand with both law enforcement and industry leaders to explore the best techniques for detection and eradication, and serves as the global clearinghouse for this effort, sharing information in a truly collaborative way.

Mr. Chairman, I don't come before you today with a quick, easy solution to the problem of child sexual exploitation, but I can state unequivocally that the advent of the Internet has provided predators with the means to both entice children into sexual acts and sustain a lucrative commercial enterprise that demands the heinous victimization of children. We suspect that the problem of child pornography will continue to increase as distributors search for lower risk avenues with a lower possibility of being detected. Federal, state and local law enforcement are more aggressive than ever before, but they must overcome significant barriers. I hope that you can help us remove some of those barriers and help us identify and prosecute those who are misusing the Internet for insidious, criminal purposes. Too many child pornographers feel that they have found a sanctuary, a place where there is virtually no risk of identification or apprehension.

NCMEC urges lawmakers, law enforcement and the public to take a serious look at the dangers threatening our children today, and to move decisively to minimize the risks posed by those who exploit new technology and target our children.

Now is the time to act.

Thank you.

The CHAIRMAN. I thank you very much, Mr. Allen. And we'll try our best to do that.

Mr. ALLEN. Thank you, Sir.

The CHAIRMAN. Our next witness, Mr. Lan Neugent, Assistant Superintendent for Technology and Human Resources.

STATEMENT OF LAN W. NEUGENT,

ASSISTANT SUPERINTENDENT, TECHNOLOGY AND HUMAN RESOURCES, VIRGINIA DEPARTMENT OF EDUCATION

Mr. NEUGENT. Thank you, Mr. Chairman.

Mr. Chairman and Members of the Committee, my name is Lan Neugent, and I am the Assistant Superintendent for Technology and Human Resources at the Virginia Department of Education, and past Chairman of the State Educational Technology Directors Association, SETDA. I am very pleased to be here today to share Virginia's perspective on education's role in protecting children on the Internet.

House Bill 58, introduced by Delegate William H. Fralin, Jr., and passed by the 2006 Virginia General Assembly, was signed into law by Governor Timothy M. Kaine on March 7, 2006. This new law made Virginia the first State in the Nation to require Internet safety to be integrated into all instructional programs statewide. The law expanded the existing statute, which was adopted in 1999. The existing statute defined acceptable use policies and practices; the new law added the requirement that the Superintendent of Public

Instruction issue Internet safety guidelines to school divisions. I do have a copy of this, and I do believe that it's in your packet.

Dr. Tammy McGraw, Director of the Department of Education's Office of Educational Technology, and her staff were charged with developing these guidance documents for local school divisions. The overall approach was to be one of balance, recognizing the need to address the rights and the risk and the highlights and the benefits of the use of the Internet in schools. We wanted this guidance to reflect our belief that the Internet offers unprecedented access to resources that can enhance learning, research, communication, exploration of new ideas, and expressions of creativity. At the same time, we wanted educators and students to understand that the dangers associated with the Internet are real, significant, and constantly changing.

To develop the guidelines, agency staff consulted with students, parents, educators, researchers, law enforcement officials, local and State and Federal representatives, and independent nonprofit organizations. These consultations, and an extensive review of research and resource materials, led to the following essential conditions regarding an effective Internet safety program:

First, Internet safety must be a shared responsibility. Children and the many adults in their lives all play important parts in ensuring safe and responsible Internet use. In developing the guidelines for schools, we identified key issues that each role in every group, from students to board members, should know.

Second thing, Internet safety must be integrated into the curriculum and be part of teachers' daily practice. Our work showed that Internet safety cannot be covered in a single lesson or a unit by use of a single program or resource. The Internet is pervasive in children's lives. Strategies for ensuring safe and responsible use must reflect the many ways in which children experience the Internet. We developed a guide to provide teachers with strategies for addressing Internet safety in the context of Virginia's standards of learning.

There are many high-quality resources available to schools free of charge; however, schools and family need to be aware that they exist. We have reviewed many excellent resources that address various aspects of Internet safety for schools and families. Our greatest challenges are helping schools identify the most appropriate resources and assuring that they have the ability to use these resources effectively to cover the full spectrum of issues.

Unlike books and other traditional resources, Internet content changes every second of every day. As a result, we routinely apprise school divisions of new developments related to Internet safety. Our information briefs provide summaries of the most current research. This is a continued process, due to the ever-changing risk of the Internet.

Technical assistance and professional development must be available to school divisions as they design locally appropriate programs for their students. Each community is unique, and Internet safety issues tend to vary greatly from one part of the Commonwealth to another. We provide technical assistance as divisions move forward with designing their comprehensive Internet safety programs. Divisions request assistance from the State Department of Education

on a wide range of Internet-related issues; most notably, they struggle with the need to balance safety and security with instructional innovation. Social networking sites and blogs have been particularly challenging for school divisions.

Virginia is fortunate to have approximately 1500 instructional technology resource teachers. These are folks who work directly with schools to help integrate technology into instruction. These highly skilled educators receive extensive professional development and support from our agency. They, in turn, provide training and support for the teachers in their schools. Library media specialists and school administrators also receive development through conferences and regional events. These educators are essential to our Internet safety program implementation. Program implementation must be monitored to assure quality and effectiveness.

To assist division superintendents, we have developed a set of rubrics—that's also in your packet—that measure the degree to which each division has adapted its acceptable-use policy and implemented an Internet safety program. These tools enable divisions to track their progress and determine technical assistance needs.

Also, public-private cooperation is essential. Protecting children on the Internet is a daunting task, as you heard from many of the speakers, that requires the commitment of everyone. We have been particularly successful in working with other organizations, both private and public, to advance Internet safety in Virginia. Attorney General Bob McDonnell launched an—Youth Internet Safety Task Force, comprised of leaders from prominent Internet companies, educators, parents, elected officials, and law enforcement, to identify solutions for the growing problem of sexual offenders and other criminals who use the Internet to target children and teenagers in the Commonwealth. This group's work has formed the basis for significant legislation and programs to advance Internet safety in Virginia.

We have also worked closely with Bedford County Sheriff Michael J. Brown on the Operation Blue Ridge Thunder Internet Crimes Against Children Task Force, as well as Jane Madison's University Institute for Infrastructure and Information Assistance, the National Cyber Security Alliance, and other organizations devoted to Internet safety and security. Furthermore, we have engaged in direct dialogues with companies to help shape their products and their services to address Internet safety concerns.

All of these efforts are converging toward one principal objective: maximizing the potential of the Internet, while ensuring the safety of each student. Safe and responsible Internet use is at the forefront of our efforts, even as we develop cutting-edge Internet applications that range from online testing to studying astronomy in the daytime through a remotely controlled telescope in Australia.

Thank you.

[The prepared statement of Mr. Neugent follows:]

PREPARED STATEMENT OF LAN W. NEUGENT, ASSISTANT SUPERINTENDENT, TECHNOLOGY AND HUMAN RESOURCES, VIRGINIA DEPARTMENT OF EDUCATION

Mr. Chairman and Members of the Committee, my name is Lan Neugent and I am the Assistant Superintendent for Technology and Human Resources at the Virginia Department of Education and past Chairman of the State Educational Tech-

nology Directors Association. I am pleased to be here today to share Virginia's perspective on education's role in protecting children on the Internet.

House Bill 58, introduced by Delegate William H. Fralin, Jr., and passed by the 2006 Virginia General Assembly, was signed into law by Governor Timothy M. Kaine on March 7, 2006. This new law made Virginia the first state in the Nation to require Internet safety to be integrated into all instructional programs statewide. The law expanded the existing statute, which was adopted in 1999. The existing statute defined acceptable use policies and practices; the new law added the requirement that the Superintendent of Public Instruction issue Internet safety guidelines to school divisions.

Dr. Tammy McGraw, Director of the Department of Education's Office of Educational Technology, and her staff were charged with developing a guidance document for local school divisions (See Appendix A*). The overall approach was one of balance, recognizing the need to address the risks and highlight the benefits of Internet use in schools. We wanted this guidance to reflect our belief that the Internet offers unprecedented access to resources that can enhance learning, research, communications, exploration of new ideas, and expressions of creativity. At the same time, we wanted educators and students to understand that the dangers associated with the Internet are real, significant, and constantly changing.

To develop the guidelines, agency staff consulted with students; parents; educators; researchers; law enforcement; local, state and Federal representatives; and independent nonprofit organizations. These consultations and an extensive review of research and resource materials led to the following essential conclusions regarding an effective Internet safety program:

Internet safety must be a shared responsibility.

Children and the many adults in their lives all play important roles in ensuring safe and responsible Internet use. In developing the guidelines for schools, we identified key issues that each role group—from students to school board members—should know.

Internet safety must be integrated into the curriculum as part of a teacher's daily practice.

Our work showed that Internet safety cannot be covered in a single lesson or unit or by using a single program or resource. The Internet is pervasive in children's lives; strategies for ensuring safe and responsible use must reflect the many ways in which children experience the Internet. We developed a guide to provide teachers with strategies for addressing Internet safety in the context of Virginia's Standards of Learning (See Appendix B).

There are many high-quality resources available to schools free of charge; however, schools and families need to be aware that they exist.

We have reviewed many excellent resources that address various aspects of Internet safety for schools and families. Our greatest challenges are helping schools identify the most appropriate resources and ensuring they have the ability to use these resources effectively to cover the full spectrum of issues. Unlike books and other traditional resources, Internet content changes every second of every day. As a result, we routinely apprise school divisions of new developments related to Internet safety. Our information briefs provide summaries of the most current research (See Appendix C). This is a continual process due to the ever-changing risks on the Internet.

Technical assistance and professional development must be available to school divisions as they design locally appropriate programs for their students.

Each community is unique, and Internet safety issues tend to vary greatly from one part of the Commonwealth to another. We provide technical assistance as divisions move forward with designing their comprehensive Internet safety programs. Divisions request assistance from the state Department of Education on a wide range of Internet-related issues; most notably, they struggle with the need to balance safety and security with instructional innovation. Social networking sites and blogs have been particularly challenging for school divisions.

Virginia is fortunate to have approximately 1,500 instructional technology resource teachers who work directly in schools to help integrate technology into instruction. These highly skilled educators receive extensive professional development and support from our agency. They, in turn, provide training and support for the teachers in their schools. Library media specialists and school administrators also

*All appendices to this document are retained in Committee files and can be found at *www.doe.virginia.gov*.

receive professional development through conferences and regional events. These educators are essential to our Internet safety program implementation.

Program implementation must be monitored to ensure quality and effectiveness.

To assist division superintendents, we have developed a set of rubrics that measure the degree to which each division has adapted its acceptable use policy and implemented an Internet safety program (See Appendix D). These tools enable divisions to track their progress and determine technical assistance needs.

Public-private collaboration is essential.

Protecting children on the Internet is a daunting task that requires the commitment of everyone. We have been particularly successful in working with other organizations, both public and private, to advance Internet safety in Virginia. Attorney General Bob McDonnell launched a Youth Internet Safety Task Force comprised of leaders from prominent Internet companies, educators, parents, elected officials, and law enforcement to identify solutions to the growing problem of sexual offenders and other criminals who use the Internet to target children and teenagers in the Commonwealth. This group's work has formed the basis for significant legislation and programs to advance Internet safety in Virginia.

We have worked closely with Bedford County Sheriff Michael J. Brown and the Operation Blue Ridge Thunder Internet Crimes Against Children Task Force as well as James Madison University's Institute for Infrastructure and Information Assurance, the National Cyber Security Alliance, and other organizations devoted to Internet safety and security. Furthermore, we have engaged in direct dialogues with companies to help shape their products and services to address Internet safety concerns.

All of these efforts are converging toward one principal objective: maximizing the potential of the Internet while ensuring the safety of each student. Safe and responsible Internet use is at the forefront of all our efforts, even as we develop cutting-edge Internet applications that range from online testing to studying astronomy in the daytime through a remotely controlled telescope in Australia.

The CHAIRMAN. I thank you very much.

And may I now call upon Ms. Christine Jones.

Ms. Jones?

STATEMENT OF CHRISTINE N. JONES, GENERAL COUNSEL AND CORPORATE SECRETARY, THE GO DADDY GROUP, INC.

Ms. JONES. Good morning, Chairman Inouye and Members of the Committee. I'm Christine Jones, General Counsel and Corporate Secretary of The Go Daddy Group.

Go Daddy's principal business is domain name registration. We are currently the largest domain name registrar in the world. We have something on the order of 22 million domain names under management. We register a domain name once every 2 seconds, or less. And every single one of those domain names has the potential to become a website that children can look at. The amount of data—as you mentioned in your opening statement, Mr. Chairman—online is simply overwhelming, and we cannot look at all of it to make sure that it's OK.

I want to make a distinction between a domain name registrar and an Internet service provider, just to make the point. For example, if you wanted to register *ChairmanInouye.com*, you could go to Go Daddy and register that name, except that I already registered it, in anticipation of this hearing, so now you can't, but, nevertheless, that's what we do.

[Laughter.]

Ms. JONES. OK. I'll give it to you at the end of the day. OK. And Mr. Stevens, you know we went through this once before, as well. A domain name—and I gave him a domain name, for the record.

[Laughter.]

Ms. JONES. A domain name is different from a traditional ISP, in that the ISP provides the access to the Internet, so through a DSL line or a cable modem or even an old-fashioned dial-up connection. The registrar provides the entrance to establishing the presence on the Internet. So, in your case, ChairmanInouye.com.

We also host a substantial volume of Internet data. That means once you build your Website, you have to have a computer to put it on. We provide those computers, and we have a whole lot of them. So, we end up seeing a lot of what Ms. Nelson and Dr. Finkelhor and Mr. Allen and Mr. Neugent talked about, on a daily basis. And we devote substantial resources to working with law enforcement, the National Center, other watchdog groups, and others, to help protect children from Internet predators.

This can be frustrating, because it seems like the number of "bad guys" is growing faster than the number of "good guys." And we count ourselves among the "good guys," by the way.

Six years ago, when I joined Go Daddy, we had one guy, one employee, working on these types of issues. Today, we have two full departments that run 24 hours a day, 7 days a week, with dozens of employees that do nothing but try to respond to issues of child pornography, child modeling, online harassment, cyber bullying, inappropriate content, outright child predators, like the one that Ms. Nelson talked about, and other issues affecting children and their use of the Internet. It is a huge and growing, menacing problem.

And, despite our efforts and the efforts of many of my esteemed colleagues here, there are still grave dangers for children who spend time online, some of which Senator Nelson mentioned in his statement.

Not one single day passes when we don't have at least one example of something nefarious happening. I mean, every single day. These include school districts calling us, asking us to remove websites where children are being harassed or threatened; parents calling us, because their children have been approached by adults in online communication communities; videotaped kidnappings—I'm not kidding you—some real, some not—that we work with the FBI on; and so on and so on and so on.

There's one very real example I wanted to share to make a point, that we must educate children and parents about the risks of sharing information about themselves online.

A few months ago, we got a call from MySpace, the social networking community. They told us that there was a website online that had about 60,000—that's six with a zero, 60,000—MySpace user name and passwords posted on the website for everybody in the whole world to see. MySpace asked us to take that website down. And we thought, OK, that sounds like a good idea, we don't want MySpace user names and passwords out on the Internet for people to see. Most of those are run by children. A lot of those children put information about themselves out there. So, we took it down.

The gentleman who ran the website immediately removed the content. We put the website back up. There was no problem with that. The entire thing lasted about an hour. But, I want to tell you, the amount of outrage and backlash that we experienced as a result of taking that down was phenomenal. To this day, there are

full-blown websites devoted to criticizing our decision for removing that content.

I don't know what people would have had us to do. Leave the user names and passwords out there, so that everybody can go stalk Ms. Nelson, like the gentleman that did that to her when she was 13? I don't know, you tell me.

Many people, I think, would simply rather that the Internet be a free exchange of ideas, with no rules and no oversight. They have little or no concern for the potential dangers this model creates for children.

Because so much of the burden, therefore, rests on parents, we would encourage the Committee to focus on ways to educate both children and parents about the dangers of using the Internet. Apparently, protecting your MySpace data with a user name and password is not good enough anymore.

I would say most major corporations want to do whatever they can to help. The legitimate ones, the ones that Mr. Allen is talking about, that his organization works with. But we need to have some tools, to be effective, as Mr. Allen mentioned in his testimony.

So, Mr. Inouye, thank you so much for the kind invitation to testify. We are grateful that this Committee is once again looking at this issue and for your leadership on this, and for recognizing that the problem of exploitation of children online, generally—and, specifically, child pornography—is a growing and unacceptable problem that must end. And we are committed to working with law enforcement to see to it that that happens.

Thank you.

[The prepared statement of Ms. Jones follows:]

PREPARED STATEMENT OF CHRISTINE N. JONES, GENERAL COUNSEL AND CORPORATE SECRETARY, THE GO DADDY GROUP, INC.

Introduction

Good morning, Mr. Chairman and Members of the Committee. I am Christine Jones, General Counsel and Corporate Secretary of The Go Daddy Group, Inc.

Background

The Go Daddy Group, Inc. consists of eight ICANN Accredited domain name registrars, including Go Daddy.com. We have over 22 million domain names under management, and are the number one domain name registrar in the world. GoDadd registers a domain name every 2 seconds or less. Go Daddy is also a large hosting provider.

A domain name registrar serves as the point of entry to the Internet. For example, Chairman Inouye, if you wanted to register the domain name *www.ChairmanInouye.com,* you could go to *www.GoDaddy.com* to register that domain name. A domain name registrar is different from a traditional Internet Service Provider (ISP), such as AOL, MSN, or EarthLink. The ISP provides *access* to the Internet whereas the registrar provides the *registration* service for .com names and the like. In short, in exchange for a fee, the ISP provides the means by which an Internet user connects to the Internet via a dial-up connection, cable modem, DSL, or other connection method. A registrar, on the other hand, enables Internet users to establish a web presence by registering a unique name such as *www.ChairmanInouye.com.*

Once *www.ChairmanInouye.com* is registered, you would need to build a website and find a place to store, or "host," that website. Again, you could go to *www.GoDaddy.com* for storage, or hosting, services. A hosting provider differs from a traditional ISP in that the hosting provider supplies space on a computer that is accessible from the Internet rather than access to that computer which is provided by the ISP.

How Go Daddy Deals With Online Child Predators

The Go Daddy Group devotes considerable time and resources to working with law enforcement to preserve the integrity and safety of the Internet by quickly closing down websites and domain names engaged in illegal activities. We work with law enforcement agencies at all levels and routinely assist in a wide variety of criminal and civil investigations. We are also quick to respond to public complaints of spam, phishing, pharming, and online fraud and work closely with anti-fraud and security groups such as the Anti-Phishing Working Group, Digital Phish Net, the National Center for Missing and Exploited Children, and CyberTipLine. Go Daddy has made it a high priority to use its position as a registrar to make the Internet a better and safer place. It is also a priority for me personally.

My staff routinely investigates and suspends sites involving child pornography and exploitation of children in many forms and degrees of severity. These include, but are not limited to, the following: 1) sites depicting children of both genders engaged in sexual acts with adults or other children; 2) sites depicting children nude or exposing inappropriate areas of their bodies; 3) sites advertising, advocating, or promoting sexual relations with minors; and, 4) sites with false or altered images depicting children in various sexual situations. Our investigations have also uncovered sites containing photographs, videos, and text descriptions; children depicted in a sexually solicitous manner; sites that claim only to be "nudist" sites, but include pictures of naked children; and, even cartoon images depicting sex acts with infants and small children. We take each instance seriously and devote high priority attention to ensuring such websites are removed from our network, as described in more detail below.

The Domain Name Registration Process

The domain name registration system is entirely automated. There is no human intervention into the process. Because many words have multiple meanings and combinations of words can be used for both legitimate and illegitimate purposes, no domain names are automatically prohibited from registration. As mentioned above, Go Daddy registers a domain name once every 2 seconds or less. This makes it virtually impossible for a human being to verify the legitimate use of every domain name registration, particularly on an ongoing basis. To compensate for this, we have developed a notification system for reporting instances of all types of network abuse, including child pornography (hereinafter, "CP"), to our Network Abuse Department.

The Notification Process

With over 22 million domain names under management, most of our data come from third party complaints or notices. The Go Daddy Network Abuse Department can receive information that a CP site may be residing on our network in several ways: 1) direct complaint from a third party via email; 2) direct complaint via telephone; 3) tip from Go Daddy employees who have either become aware of, or suspect the existence of, CP on a customer site; and, 4) notifications from CyberTipLine and other "watchdog" groups.

The Investigation Process

Once Go Daddy is made aware that a potential CP site is registered through Go Daddy, we immediately investigate to determine whether there is CP content, and if so, whether that customer has other domain names resolving to the site with the CP content, and whether there are other hosting sites in the customer's account which contain CP content.

In many cases, Internet users can only access CP content by supplying a paid-for membership user name a password. While we cannot investigate content that requires payment to access, we do investigate all web pages found to be freely accessible to Internet uses without a user name and password for any site that we suspect may be involved in CP. If the site is hosted by Go Daddy, we may also access content directly in the customer's hosting account to ensure we eliminate all CP content. Often, the operators of websites of a pornographic nature are guarded about images on publicly accessible landing pages and store the most offensive content in directories that site visitors can only reach with payment.

After we determine that there is content meeting the criteria for classification as CP, we archive a screenshot (in the case of a registered domain) and all or partial content (in the case of a hosted site) sufficient to demonstrate evidence of CP for future use in law enforcement investigations.

The Reporting Process

Once Go Daddy's investigation is complete, we report the offending domain names, websites, and registrant information to law enforcement. We give law enforcement a short time period to request that we leave a website in tact to assist

in their investigations. This allows authorities to expeditiously gather screenshots, downloads, WHOIS data, and other information necessary for further investigation. We also report the offending domain names, websites, and registrant information to the National Center for Missing and Exploited Children (NCMEC) via their online submission and complaint area, CyberTipLine.

The Suspension Process

After the offending domain names, websites, and registrant information have been investigated and reported, we permanently suspend our services. It is important to note that domain names are not suspended prior to the investigation and reporting processes, especially where domain names are not associated with an active website. It is very difficult for us to suspend a domain name before it is associated with an active website because many words have multiple uses. And, if there is no CP content associated with a particular domain name, there is no reason to suspend the domain name itself because there is nothing unlawful about a domain name, in and of itself.

How Go Daddy Deals With Private Domain Name Registrations

Go Daddy offers privacy services for domain name registrations. A private domain name registration is recorded through a proxy registrant. This enables a domain name registrant to avoid publication of their personal information in the public WHOIS data base. We find that most of the users of the private registration service are legitimate users; bad actors typically do not want to pay extra to hide their WHOIS data when they are probably going to provide false WHOIS data, anyway. Most CP sites do not have privacy protection on them. More often, the registrant simply provides false, but valid looking, WHOIS data, upon registration.

The registration process for a domain name is exactly the same regardless of whether the customer chooses to enable privacy. While we do not have different rules for registering a domain name with privacy, we do use our Universal Terms of Service broadly to cancel privacy when the Go Daddy Abuse Department determines it is being used for ANY improper purpose. Go Daddy also gives law enforcement the proxy registrant information on private domain name registrations when they are investigating a domain name with privacy. In the case of a CP site, this information is voluntarily provided to law enforcement during the notification process described above.

Child Pornography Statistics

Go Daddy investigates thousands of domain names and websites each year for CP. The number of unique customers investigated in the past twelve months was approximately 1,500. (This number does not include the child modeling sites discussed below which are growing in numbers daily.) The number of domain names investigated each year is much higher than the number of unique customers investigated. One unique customer may have many domain names in one account. Once we find out about potential CP in a customer's account, we look to determine what other products they may have associated with CP. Many times, one customer will have literally hundreds of domain names on account. In those cases, we suspend ALL the domain names with CP, not just the one upon which we received a complaint or notification.

Importantly, these numbers are skewed slightly lower because many times when Go Daddy is the registrar, but not the hosting provider, the website content has already been removed by the hosting provider by the time we conduct our investigation. This is a result of third party complaints being sent to both the domain name registrar and the hosting provider at the same time. This is a sign that many hosting providers take complaints of CP as seriously as we do and we are, of course, grateful when we find that they are fully cooperating with us to rid the Internet of CP content.

Approximately 70 percent of the sites we suspend are registered, but not hosted, with Go Daddy. This means that in about 70 percent of the investigations we conduct, we find that the website content itself is stored by another hosting provider and Go Daddy provides the domain name registration service only. Approximately 80 percent of the CP websites we investigated in the past year were registered to an individual or company in Eastern Europe. The most common areas were Russia, Ukraine, and Romania. Importantly, the majority of CP sites we investigated in the past twelve months were registered fraudulently. This makes identifying the exact nation of origin difficult, and brings into question the reliability of numbers we collect.

How Go Daddy Deals With Child Modeling Websites

Much like CP websites, we routinely investigate and suspend sites involving child modeling. These include, but are not limited to, the following: 1) images of underage children posing in a manner intended to be explicitly sexy. (*e.g.,* emphasizing genital areas or posing in situations easily identified with sex); 2) images of underage children in adult lingerie; and, 3) images of children in states of partial nudity or very little clothing not associated with normally acceptable situations. Images of a child in a bikini swimming at a pool would not be considered. Images of the same child in a thong bikini laying on a bed and spreading her legs would be.

As these sites typically do not rise to the level of technical CP, we classify these sites as "morally objectionable," a term taken from our Universal Terms of Service. We tend to be more aggressive than most registrars on child modeling sites. We typically remove them, even if we can't find CP, because our experience has been that the operators of child modeling sites tend to be associated, even if attenuated, with CP in some way. We also remove the non-traditional forms of CP like nudist sites and cartoon CP.

The Domain Name Registration Process

While there is no prohibition against registering a child modeling domain name (because there is nothing illegal about the domain name itself), we do treat child modeling websites in a manner similar to CP sites. We have seen child modeling sites with more and more frequency over the past year. Almost every time we find a child modeling site, we learn that the customer has multiple domain names specializing in child modeling. We also find that a customer who runs child modeling sites typically also has CP on its site somewhere, or that the child modeling sites lead, even if circuitously, to CP on another site the customer controls somewhere. Based on our investigations, we have found that the vast majority of these sites are of little girls.

The Notification Process

All child modeling website investigations originally come in as notification of alleged CP (as described above) by third parties or employees. When we are notified of a child modeling site, it is transitioned to a child modeling investigation as soon as it is discovered to be a child modeling site not containing explicit pornography.

The Investigation and Reporting Process

We follow nearly the same procedure for child modeling sites as described for CP investigations. Because the child modeling sites fall squarely under the charge of the NCMEC, as they are clearly exploiting children, these sites are also reported to the NCMEC.

The following example demonstrates the importance of all ISPs, registrars, and hosting providers taking child modeling sites seriously. One child modeling investigation we conducted recently uncovered a registrant engaged in CP. We discovered this particular customer had over 200 domain names attached to active child modeling websites. After following our standard investigation procedures, Go Daddy submitted their information to authorities. Two weeks later, this customer was arrested and indicted on multiple counts of CP. This is just one of many examples of a direct link between information we have provided and arrests for CP.

Child Modeling Statistics

We investigate thousands of domain names and websites each year for child modeling. The number of unique customers investigated in the past year was approximately 780. As with CP, the number of domain names investigated each year is much higher than the number of unique customers investigated. This is because one unique customer may have many domain names in one account. Many times, one customer will have literally hundreds of domain names in its account. In those cases, we suspend ALL the child modeling domain names, not just the ones upon which we received a complaint or notification.

Approximately 60 percent of the sites we suspend are registered, but not hosted, with Go Daddy. This means that in about 60 percent of the investigations we conduct, we find that the website content is stored by another hosting provider and Go Daddy provides the domain name registration only. This statistic might tend to suggest that child modeling operators are more comfortable using the services of a mainstream hosting provider than those who engage in pure CP, although we have no independently verifiable data to support that suggestion. Approximately 60 percent of child modeling websites we investigated in the past year were registered to an individual or company overseas, typically in European countries. Unlike with full blown CP, approximately 40 percent of child modeling sites we investigated and sus-

pended in the past twelve months were registered to an individual or business in the United States.

Conclusion

Thank you, Chairman Inouye, for the kind invitation to testify today regarding protecting children on the Internet. We are grateful for this Committee's attention to this important issue and for recognizing that the problem of online exploitation of children generally, and child pornography specifically, is a growing and unacceptable menace that must end. Go Daddy is committed to taking whatever steps are necessary and feasible to assist in ending this practice, and we would challenge our counterparts on the Internet to make the same commitment.

The CHAIRMAN. Thank you very much, Ms. Jones.

Senator Stevens?

Senator STEVENS. Thank you very much. I would not be able to come back after the vote, so I do thank you, appreciate the opportunity.

I'm interested, Ms. Jones, in the question of whether or not the community out there dealing with the Internet in general has any idea of what type of an education program would work.

Ms. JONES. There are many conversations that happen around this issue. And, as Mr. Allen said, there's not one single silver bullet, there's not one single simple solution. But, if you teach a teenager not to post pictures and not to put their address and phone number, not to put their hometown on the Internet, those kind of simple solutions—I mean, basic, fundamental stuff—that would go a long way toward helping kids escape some of the predators that are out to get them.

I think Ms. Nelson made the point, people on the Internet go after the weakest link. They want the kid that's easy to get. So, if each child knows, "Hey, you know what, if you're going to be on the Internet, don't put your stuff out there," that would go a long way to solving the problems that we're talking about right now.

Senator STEVENS. Is there any way that you think that the system could be modified so that parents would have greater control over children?

Ms. JONES. Well, there are some proposals around that issue, for example, the dot-US [.us] country code top-level domain, which is central to the United States. They have an area called dot-kids-dot-US [.kids.us], which is supposed to be used specifically for children on the Internet. That type of thing would work for smaller kids. Teenagers, they're not going to buy it, right? Because they want to go out, and they want to explore, and they want to do their own thing. But, if you had some areas that were defined so that parents could know and monitor and get feedback and reports on every single spot that their kid went to, every single chat conversation they had, every website they viewed, I think the parent would kind of get the idea, if they know their kid was talking to some kind of strange-sounding person in another State. That is pretty simple to implement. Getting the word out and helping people to understand that that's available, that's the educational process that we're talking about.

Senator STEVENS. Is there agreement on the panel that the real problem is in the sub-teens, rather than in the teen level? Teens have access to a lot more computers in school and in clubs and everything else. I think the sub-teen level ought to be the main target of any legislation. And is there agreement on that?

Dr. FINKELHOR. I guess I would say no. I think that, while it's important to educate the preteens about the dangers that they can encounter online, I don't think that they are quite yet ready to understand some of the kind of risky activities that will really get them into a lot of trouble. I think this has to go along with some of the information that we give them when they start to be interested in romance and taking risks, so that there's a different kind of educational package that we need to target at those teens, and particularly at these teens who are inclined to take risks and who may be having serious problems in their——

Senator STEVENS. I was talking more about parental control. It seems to me we could put some parental controls on home computers, but I don't think we can go out to the stores and other places where teenagers can access the Internet somewhere. The sub-teens really don't have that opportunity.

Anyone else comment on that?

Ms. Nelson, what do you think?

Ms. NELSON. I feel, as Dr. Finkelhor said, I think that we can educate our teens on ways to stay away from predators, but I feel that education of safe Internet usage should start a lower level. Kids as young as 5 and 6 are using the Internet. If they knew simple habits, like, "Don't talk to strangers," just like you don't on the street, "Don't share your personal information, involving adults if you feel uncomfortable," if they know those habits at a younger age, they will learn to be more responsible Internet users as they grow with age.

Mr. ALLEN. Senator Stevens, let me add, I think there's no question that educational emphasis has to be put on the sub-teen group. Teens are tough. And what we've tried to do, what many of the groups that are doing such great work in this area have done is try to look for that way to really communicate with teens on their level, that they understand. The second part of the message is to parents, "Your parenting obligation isn't over just because your kid's 13 years of age. They're not virtual adults, they are still kids." I think we have to continue to pound home the message on parents that, "You need to be involved in your kids' lives, you need to talk to them and communicate with them, and make sure you understand the kinds of challenges they're facing."

So, I think the answer, unfortunately, has to be multifaceted, comprehensive, and target both age groups, and keep parents in the mix.

Mr. NEUGENT. If I may add to that, in education what we've found is that many of the teachers that are working with children don't have all of the skills that are necessary to help protect them, and that's why we're developing the Internet curriculum, so that they can take a look at that. And we do find it pervasive, all the way from kindergarten through high school. There are unique issues with every age group, and the guidelines and the things that we're working on are to try to make it so that all of those areas have some influence over that. The role of leaders, the role of administrators in school, the role of the people that influence children's lives, is critically important as they start to work with it.

One of the things we're trying to do, for example, is to educate parents so that they understand how to check a log and see where

children have been, just as many of the panelists have said, sometimes a simple thing like that, parents just don't know how to do that, and can't track where their children have been.

Senator STEVENS. Thank you very much.

Thank you, Mr. Chairman.

The CHAIRMAN. Thank you.

Senator Nelson?

Senator NELSON. Thank you, Mr. Chairman.

We know, on the basis of Mr. Nugent's testimony today, what they're doing in Virginia with regard to education. And I'd like to ask the rest of the panel, what do you think are the kind of programs that will work the best in order to educate children as part of the overall curriculum?

Ms. NELSON. As I said earlier in my testimony, they have the opportunity to be a part of computer classes, as young as the middle-age schooling. Taking time during those computer classes to implement Internet safety education is one of the ways that I feel that it would be most effective, because they would be made to learn about the issues of the Internet. Kids aren't always going to want to hear these stories, they're not like Ms. Jones said, they want the Internet to be a free place where they can express themselves. But if they're made to learn about it, if they're made to be safer Internet users, they will learn these rules a lot easier.

Dr. FINKELHOR. I'd just like to make another pitch for what I see as crucial here: research on this issue. I'm not sure that we know what the best prevention message is. I'd like to highlight some missteps that were made many years ago with the drug-use problem. We ran in, in response to the sense that kids were taking drugs, and tried to scare them off. And it turned out not to have been very effective. And it took us a decade or more before we understood that we had to go in and teach kids specific drug-resistance techniques, and help them by role-playing these skills.

Senator NELSON. Well, do you think that——

Dr. FINKELHOR. And we need to go through that same process——

Senator NELSON. Do you think Virginia——

Dr. FINKELHOR.—to try to do it earlier.

Senator NELSON.—is on the right track?

Dr. FINKELHOR. Do I think what?

Senator NELSON. Virginia is on the right track?

Dr. FINKELHOR. I'm not familiar, entirely, with what they're doing, but my sense is that a lot of the messages that we've got are based on hunches about what would work, but we really haven't roadtested them yet to see if they actually get kids to be safer online.

Senator NELSON. Mr. Allen, you mentioned a number of additional tools that you'd like to see Congress give to law enforcement. Of those proposals, which are the one or two that you think are the most important?

Mr. ALLEN. Well, the two that I think are the most important, Senator Nelson, is—one, I think the Congress needs to fix the 1998 law that mandates Internet service providers to report child pornography on their system. The good news is, the major players are

doing it willingly and aggressively. I think that's a problem that is fixable by statute and needs to be fixed.

The second thing is, I think there is a huge challenge for law enforcement in terms of the connectivity information. I know that's a complex issue, with—certainly with the ISP community. I'm convinced there is a reasonable resolution that does not go after content, but just requires preservation of those connectivity logs.

And third—and I know this is the Commerce Committee and not the Appropriations Committee, but I think law enforcement needs help. Somebody said earlier, the sheer scale of this problem far exceeds anything that we anticipated, and Federal law enforcement, the FBI's Innocent Images National Initiative, ICE, and the agencies that are attacking this problem, need resources. State and local law enforcement needs resources.

Senator NELSON. Mr. Chairman, I just want to agree with your comments about the young lady providing testimony. And I want to say that, Ms. Nelson, you're in a unique position because of what you have been given, the title, in order to have a great deal of influence on a lot of people. And the fact that you have chosen this as your subject area, I think, should indicate the highest of compliments from us, who are concerned about this.

Thank you.

Ms. NELSON. Thank you very much, Senator.

The CHAIRMAN. Thank you very much.

Senator Rockefeller?

Senator ROCKEFELLER. Thank you, Mr. Chairman.

I'm a little bit mystified by the whole concept of educating parents and educating children, as opposed to stopping the activity, in the first place, through law.

There was a instance recently here where the movie industry spent $250 million—not of their own money, I might add—of trying to convince Americans that they were doing the best that they could on indecency, and how to use the V-chip, and all those kinds of things. And it was a predictable failure. It was a predictable failure.

I agree with, I think, with what you said, Ms. Nelson, that if people—if children—young people feel they're being talked down to, or they're being "educated" to achieve a higher moral standard in, sort of, a special circumstance, they're less likely to listen. I think parents are more likely to listen, but parents, on the other hand, are less likely to understand what the problem is, except as their generation is younger and they're more familiar with it.

I mean, for example, 85 percent of parents, which is certainly the overwhelming majority, claim to have implemented rules in their homes about Internet sites their children can visit. Implemented rules. That's definitive. And, additionally, a majority of parents, 53 percent, claim to have filtering software to limit access to certain Internet content. Again, that would seem to be a case-closed type of activity. But then, at the same time, 70 to 90 percent of children claim to have viewed pornography online, much of it graphically very hardcore. So, on the one hand, we educate, or we give people either—in the case of television, V-chips or Internet—other types of ways of blocking. And, on the other hand, it doesn't seem to work. So, I think this is the conundrum. There's no single bullet.

I think what appeals to me the most is what you suggested, and that is making it part of the curriculum. I don't know, what do you have, a 45–50-minute Internet class, and little kids start, you know, at 4 or 5 years old, or 3 or 4 years old, and they start, and then they get better at it. But they always have that available to them. And I think it ought to be—just as we don't teach physical fitness anymore, maybe we could substitute mental stability for physical fitness, and at least not have people fall into those types of situations.

I think children respond to what they learn in the classroom, because it's sort of like math and science. I mean, it's likely to be right. What you're told is likely to be right, or at least it's a point of view which is given to you by a figure that you respect who's not threatening to you—that is your teacher—as opposed to your parent, who can be put into that position.

So, on the other hand, I have no idea that that will work either. I have no idea that that will work either. And I just wonder, several of you made your remarks, and you said we've got to do more of this and more of this and more of this, and nobody really got, again, back to the people who are actually doing it. It was a question of how to stop something from appearing on the Internet, stopping opportunities for children to be able to do things they shouldn't, but not foreclosing—you were different, Ms. Jones, when you talked about getting rid of some of these sites, and then all of the backlash, which I find absolutely fascinating, which I think underlines the problem of the voracious hunger for this kind of stuff, which ought to be extremely scary to all of us.

But, to me, if you don't want to have bad language on family programming, which is now described as 7:00 to 10:00, and children's hours are 7:00 to 10:00, and which we all know is ridiculous. I mean, children start their homework at 10:00. And so, they get to see all the bad stuff, even while we're preaching the 7:00-to-10:00 concept. So, isn't it—actually making it a part of the curriculum—I don't know what you do about parents, because I think parents are a very mixed group. Some want to, but don't know how to. In the case of the Internet, obviously, if you come from a rural State, West Virginia, like I do, there are a lot of parents who don't know how to use the Internet, so they wouldn't have the first idea of how to tell their children about what to do, or there is no Internet connection at home. In the classroom, yes; at home, no. I think a lot of parents are also afraid to appear to be moralistic in such direct, "You can do this, you can do that, I'm going to block this, I'm going to block that, this is why I'm going do it." And so, that's a hard thing for—it's a hard intervention for a parent. It's a necessary intervention for a parent, but, on a human basis, it's a difficult one for them to make.

So, my feeling, still, is that you put this into the education, you make it part of the training, and you don't make it just for 1 year, you make it all throughout, so that whether you're dealing with 5-year-olds or 15-year-olds, they're all children, and they're all subject to different people's, you know, malevolent interests. And then, second, finding ways to close legal loopholes, to raise fines, or simply to make something illegal, to make something criminal. I mean, if there's anything that's criminal, it's the attacking of a young

child, even the attracting of a young child. It's a criminal activity, as far as I'm concerned. Now, I'm not a lawyer, it may be treated as such, but I don't think so. So that I think sometimes we're too delicate in the way we try to approach things. Education is a very long-term process. There are a lot of people that don't know a whole lot about Shakespeare, and we've been teaching Shakespeare for two or three hundred years.

So, I'd just like to have you react to my point; that is, number one, you make it a part of the curriculum, so that the children themselves ingest in an atmosphere which they can trust and feel comfortable with, surrounded by their peers, therefore no bullying, as to how they can get into trouble; and then, after class, they discuss how some of them did get into trouble. And so, it sort of feeds upon itself, on the one hand; and, on the other hand, action which strikes down the profitability factor, not just closing in on the records, but figure out ways to make it impossible for people to do it.

Mr. NEUGENT. Mr. Rockefeller, before others respond, if I could just say that, in your packet is Virginia's Internet Safety Guidelines Curriculum. We certainly concur with what you're saying, Internet safety instruction needs to be in the schools, it needs to be in all of the curricula areas. And you'll see examples in all of the major areas in Virginia.

Senator ROCKEFELLER. Is it done every time an Internet class is taught, is it done? Is it done three times a week? Is it done once a week? Is it a regular part? Does it go on for 10 or 12 years? That's what I'm interested in.

Mr. NEUGENT. Yes, in all of the curricular areas.

Senator ROCKEFELLER. It just never gets—you never can get away from it in school.

Mr. NEUGENT. This is a shared responsibility of all teachers. That's the way we work with Internet safety in Virginia, so that a teacher in kindergarten, first grade, a history teacher in ninth grade, all have a shared responsibility. And what we've tried to do is to show them, against our standards, those things that they should do in each of the curricula areas.

Senator ROCKEFELLER. And then they have to do it.

Mr. NEUGENT. They have to do it.

Senator ROCKEFELLER. And then, are they monitored by the——

Mr. NEUGENT. Also in your packet is a monitoring document to check and see that it is being done.

Senator ROCKEFELLER. Any other——

Mr. NEUGENT. I don't think it's something we will have an answer to immediately, but certainly the monitoring document will give answers over time——

Senator ROCKEFELLER.—comments?

Mr. NEUGENT. I don't think it's enough, it's just a start, but I know we will do more in the future.

Senator ROCKEFELLER. No, no, it's——

Dr. FINKELHOR. I agree with what you're saying, and I think that broadening the approach across the curriculum is very important. There's an additional broadening dimension, in addition to talking about Internet safety: we need to be talking about Internet citizenship. We can take a lesson from the community policing and crime

control experience. When communities were able to mobilize neighborhoods into Neighborhood Watches, where everybody felt a kind of responsibility for what was going on, reporting things that they saw that were disturbances, behaving well themselves when they were in public spaces, we cleaned up a lot of neighborhoods. And I think the Internet is a kind of neighborhood too, which needs this kind of Neighborhood Watch kind of orientation. And that's something we can be also addressing in this curriculum that you're talking about.

Senator ROCKEFELLER. Mr. Chairman, will you yield me an additional 30 seconds?

The CHAIRMAN. Proceed.

Senator ROCKEFELLER. I want to disagree with that. I don't want to say it's a bad idea, but, to me, there is such an enormous difference between the Neighborhood Action Committee, between breaking and entering and permanently either scarring a child's mind or damaging a child, which is a criminal activity of an entirely different dimension. I meet regularly, when I go back to West Virginia, with students and parents and psychologists and others, and school officials, and we talk about that. Their view is so one-sidedly in favor of cracking down, it's not even funny. And I don't pick them out to reflect the way I think about it, they just show up. I mean, they're angry about this, and they feel helpless about this. And if the parents have tremendous Internet capacity, that's terrific, but most of them don't feel confident, or they don't feel confident how to approach their children on this thing. And I think it has to be a really targeted one-on-one type of thing.

Thank you, Mr. Chairman.

The CHAIRMAN. Thank you very much.

Senator Klobuchar?

STATEMENT OF HON. AMY KLOBUCHAR,
U.S. SENATOR FROM MINNESOTA

Senator KLOBUCHAR. Thank you, Mr. Chairman.

Thank you, all of you, for coming.

And I know Mr. Allen well, from the work he's done, as a former prosecutor. We've worked together.

And I will say that I look at this just from, first, as a parent, the challenges I've had. I remember the last 2 years, the only campaign question that stumped me was at a teen program. They asked me if I knew what "LOL" meant. Do you know what that means——

Ms. NELSON. Laugh——

Senator KLOBUCHAR.—Ms. Nelson?

Ms. NELSON.—out loud.

Senator KLOBUCHAR. Exactly, laugh out loud. Well, I didn't know that, and my daughter, who's 12, reminds me of that every day.

And one of the things I think we see is that these kids are ahead of us on the Internet, and it means that we have to learn what we're doing and make sure those standards are in place. And I've been impressed by some of the work you've done, Mr. Allen, on that, as well as the rest of the panelists.

The second way I look at this is as a former prosecutor. And I saw these horrific cases that we had, where we would trace them

back—rapes or other cases—to where young people had met people over the Internet. And we had a number of child porn cases, as well. And one of the things I always reminded our people was that these child porn cases, while it's a crime itself, there's something sort of distant about it, where it doesn't seem real, but it became very real to us when we had a case where it was just a child porn case, actually, against a professor. I remember, his name was Professor Pervo——

[Laughter.]

Senator KLOBUCHAR.—and he had been looking at hundreds of images of porn. He was prosecuted. There were some pictures, so we were trying to figure out, Are these real kids? Do they live in Minnesota? Can we help them at all? And we saw—one of the pictures had a high school—some kind of emblem in the back, and the police traced it, and they found a kid in a small town in rural Minnesota who had basically, been molested, and he somehow had ended up in this grouping of pictures that this professor had as a series of pictures of child porn. And it reminded me again that these are real children who are real victims of crimes, and not just images on the Internet.

So, I look at this in terms of law enforcement. My questions are more along that vein. First of all, I know that we've had some concern in investigating these cases, about the data retention policies of some of the Internet service providers, that they're inadequate, and sometimes we're unable to get the information we need. And I guess I'd ask you, Mr. Allen, or anyone else that could shed some light on this, What is the average time that ISPs retain this information? And what do you think would be an appropriate amount of time?

Mr. ALLEN. It varies widely, and that really is the problem. There are a number of companies that have been extending that retention period 30 days, 60 days, 6 months. From the law enforcement folks that we talk to, in our view it needs to be at least a year, preferably longer. And, again, our accommodation, recognizing that this has real impact on these companies if they're required to maintain massive amounts of data, our view is that what they should be required to retain are the connectivity logs. The key issue for law enforcement is, you have to establish that this person went online at this time from this particular site. I think there is a way to resolve this conflict without devastating the industry. But we hear it from our law enforcement partners across the country every day, you can't make the cases without that basic information. We really have to resolve the whole data retention issue.

Senator KLOBUCHAR. And the other piece of this, which you touched on is the training of police officers. I just remember some cases we had early on with small police departments, where they'd come upon a scene and were investigating a child porn case. And sometimes there aren't big rings, it's just one person or they're trying to figure it out, and they get to the computer, and they start turning it on, themselves, and turning it off, and basically there were triggers in there that would ruin all the evidence that we had. And we did some training videos on this that were really basic. But I remember, at some point, the Federal Government was offering to do these regional investigations to help local law enforcement

with forensics and other things. And I just wondered what the status is of that. It's clearly a problem for local police departments.

Mr. ALLEN. It's a huge problem. We, at the National Center, are bringing law enforcement in, as well as going out to do these kinds of training programs. A real step forward in all this has been the creation of the Internet Crimes Against Children Task Force Program. Your ICAC in Minnesota has been terrific, and has made lots of cases.

Another major challenge in this area is the whole issue of forensics, because computer forensics are very demanding, are time consuming. If you seize a computer that has 60,000 images on it, it's going to take time to get that. I've talked to FBI leadership about it. One of the big challenges now is, it's just taking too long to build these cases. I know there's a dollar sign attached to that, too, but we've really got to pay more attention to building forensic capability targeted to this kind of issue.

Senator KLOBUCHAR. And my last question is, Is there technology currently on the market or in development that can catch perpetrators who rely on this peer-to-peer file-sharing networks to traffic in child pornography?

Mr. ALLEN. The answer is yes, but this is an evolving proposition. One of the real challenges here, as you know from your time as a prosecutor, is, like every other aspect of human life, the bad guys tend to get the new technology before law enforcement. So, we've spent 10 years trying to help law enforcement catch up. And what we're seeing now is that, when you make headway in one area, the technology evolves. So, it is a continuing process.

I think the most encouraging thing is that these technology companies want to help. For example, we are now working with AOL, Microsoft, Yahoo!, Google, EarthLink, and United Online in an effort to develop a database of hash values. Basically, each one of these images has a fingerprint; and a lot of the images on the Internet are not new images, they circulate forever. So, one of the things we're trying to do is work with technology companies to try to develop new technologies to identify and interdict those identified illegal images and keep them from reaching the computers of America's consumers.

Senator KLOBUCHAR. Thank you.

And I also wanted to thank you, Ms. Nelson, for being here. I must tell you that we had a case once when I was a prosecutor, a white-collar case, and one of your predecessors testified in favor of the defendant, because she was his friend, that he should get a lighter sentence. And I was always telling the story, for years, that we took him on, even though the former Miss America testified on his side, and that it didn't bother me, because I was a former Miss Skyway News of March 1988.

[Laughter.]

Senator KLOBUCHAR. So, I'm just so pleased that you are on our side, testifying on this issue, so that you've righted the name, in my mind.

Ms. NELSON. Well, thank you.

Senator KLOBUCHAR. Thank you.

The CHAIRMAN. Thank you.

Senator Pryor?

STATEMENT OF HON. MARK L. PRYOR,
U.S. SENATOR FROM ARKANSAS

Senator PRYOR. Thank you, Mr. Chairman.

Let me start, if I may, with Dr. Finkelhor. In your testimony, and in your written testimony, you say that—I guess you come to the conclusion that giving out personal information or participating in social networking sites is not the most crucial factor that places children at risk. Is that fair?

Dr. FINKELHOR. That's right.

Senator PRYOR. All right. I'd like to ask Mr. Allen if you agree with that statement.

Mr. ALLEN. We think that putting personal information out there puts kids at risk. I think what Dr. Finkelhor is saying is that—I won't speak for Dr. Finkelhor—but that there are other factors that appear greater.

We think there is abundant evidence, including Dr. Finkelhor's research, that indicates more kids are posting personal information, more kids are posting photographs today than ever before. His research indicated that kids are being more cautious. Fewer kids are interacting with people that they don't know. But, in our judgment, it puts kids at risk, and that we should continue to work to stop kids from doing it.

Senator PRYOR. Dr. Finkelhor, do you agree with what he just said?

Dr. FINKELHOR. Well, I think it's a generally good idea to tell kids, "Be judicious about what you do with personal information, because you don't know where it's going to end up or who's going to use it." But our research does suggest that it's the exchange of personal information, the posting of certain elements of personal information, like your Web address, and things like that, are so widespread. And our research suggests that that's not an indication of the kids who are actually getting solicitations and getting into trouble.

The parallel, I think, to make is with kids being out on the street say, walking to school. It's probably the case that if you never walk to school, your chances of getting abducted are reduced somewhat, because some kids are going to get pulled off the street. But there are other reasons to be on the street. And it's not a big factor. What's most important is to talk to kids about what to do when they get approached, how to not play into the hands of the solicitors and the predators there. If we think that we're making kids safe by just telling them, "Don't post information, don't talk to anybody you don't know," that that's not going to really take them very far on this road to protecting them.

Senator PRYOR. All right. Well, just to be clear for the Committee, in your opinion is the Internet fostering an increase in inappropriate contact between adults and minors? Is the Internet adding to the problem, or is it a net neutral?

Dr. FINKELHOR. Well, that's a really good question, because it would seem as though adults have greater access to kids on the Internet, and the Internet has provided a kind of community forum for people who have these deviant sexual interests, to kind of communicate with one another, maybe even learn from one another. But an interesting fact is that, during the same period when the

Internet was penetrating into so many households over the last 10–12 years, sex crimes against children have actually been declining in this country.

Senator PRYOR. So, is——

Dr. FINKELHOR. And I'm not sure that it's the Internet that has caused that decline. In fact, I don't think it's really been a part of it. But it seems to me a mistake to jump to the conclusion that the Internet has made kids much more vulnerable to sex crimes than ever before, when you see this decline in overall sex crimes.

Senator PRYOR. All right. In your opinion, then, is it fair to say that child predators have, kind of, moved from the shopping malls and the playgrounds and et cetera, et cetera, ball fields, et cetera, to the Internet?

Dr. FINKELHOR. No, actually—for the people we consider pedophiles, that is, people who have a primary sexual interest in prepubescent kids—they really don't get much access to kids online. Those kids, at that early age, are really not interested in communicating with people online. These pedophiles have to go through the traditional social networks to access kids. What it has, perhaps, increased is access to teenagers, and particularly those teenagers who are vulnerable because they're in turmoil in their lives and in search of romance and affection and understanding.

Senator PRYOR. Interesting.

Mr. Allen, let me ask you—and it's good to see you again, by the way—but let me ask you about—you mentioned something—I believe it was Senator Bill Nelson, here, a few moments ago—about the statute needs to be updated, needs to be fixed. Could you give the Committee some more of your thoughts on that? What do we need to do to the statute?

Mr. ALLEN. Well, the Congress mandated Internet service providers to report, but regulations have never been issued by the Justice Department. The law was passed in 1998. And, while we have worked with the companies voluntarily—327 companies are reporting—the position of the Justice Department has been that this was a flawed statute that's essentially a civil statute with a criminal penalty; and, therefore, for "intent" reasons, nobody's ever been sanctioned under the statute. Our view has been: If the statute is flawed, we ought to fix it; we ought to amend it.

And so, simplistically, the code section is 13032, and we believe it's time—we think this is an important tool. These reports have led to hundreds of successful arrests and prosecutions. And what we have learned, anecdotally—I mean, we've handled 500,000 reports, but, of the cases that we have handled from these reports from the ISPs, we are learning that these are overwhelmingly not instances in which people are just downloading images and looking at the pictures; these are people who are downloading images, looking at the pictures, fantasizing about it, and then acting physically against real kids. So, we think this is, in the scope of things, I'm sure it's not as big as some other issues, but we think it's one that is yielding real dividends, and our concern is that, if there are only 327 ISPs reporting, what we don't want to see is smaller ISPs become safe havens for this stuff. So, our recommendation is that that statute be amended so that regulations can be promulgated,

and every electronic service provider be mandated to report. And if they don't, they should be sanctioned under the statute.

Senator PRYOR. Well, I'd like to work with you on that. If you all have some language or some—you know, if we can get down and really look at the statute and try to come up with some specifics, I'd really like to work with you on that.

Mr. ALLEN. That would be great.

Senator PRYOR. So, please be in touch on that.

And the last thing, Ms. Jones—and I know I'm out of time here, but—parental controls. Are parental controls the answer? I mean, it seems to me—I have a bill that, you know, really tries to do a better job of identifying images, et cetera, information out there that we don't want young people to see and be exposed to. But how important is the parent in this process? And what is some of your practical advice of things we can be doing, or should be doing, as a Congress?

Ms. JONES. There's no simple answer to that question. Parental controls are not "the" answer. Parental controls are "an" answer. Amending the 1998 statute so that my colleagues in the hosting community actually provide data to Mr. Allen's organization is "an" answer. Getting out and implementing something like what Virginia has in schools in schools is "an" answer. But I cannot overemphasize the importance of parents being involved in this process, because if your kid is sitting in their bedroom looking at the Internet, and you don't know what they're looking at, chances are they're looking at something bad, just like everything else your kid does in the bedroom with the door closed without you knowing about it. Kids push boundaries, and so, the parent has to be involved.

Some parental controls that are available work. Some of the filtering works. If the technology coalition that the National Center has put together actually gets this database of known images, that will be hugely helpful. I can go bump up against our database of thousands upon thousands upon thousands of computers with millions of hosting accounts, clean the entire thing of every image that's in that data base. That's a filter. That's helpful. But the parent has to put the filter on the computer of the kid that's looking at it in order for what I just did to make it effective.

I think no matter what we do, it's always going to come back to the user. And I know Senator Rockefeller was uncomfortable with that, because it seems like we're putting the burden on kids and parents to do the right thing, and we're letting the criminals run free. That's not the case at all. We get phone calls every single day from law enforcement all over the country who are pursuing the "bad guys." Yesterday, in Florida, 22 people were arrested in a case that we helped with in a child pornography ring. That stuff is also happening—that's another sort of parallel line that's going on. But you've got to have the parents involved. I cannot overemphasize it. And if you're a kid, and your parent doesn't know how to use the Internet, teach 'em how to use it.

Senator PRYOR. Thank you, Mr. Chairman.

The CHAIRMAN. Thank you.

Senator Cantwell?

STATEMENT OF HON. MARIA CANTWELL,
U.S. SENATOR FROM WASHINGTON

Senator CANTWELL. Thank you, Mr. Chairman.

And thank all the panelists for being here, and, Mr. Chairman, for holding this Committee.

Could we talk about statistics for a minute? Because I know that some were mentioned, but I want to understand—I think, in 2004, there were reports of 200,000 online child pornography cases. Do we know, Mr. Allen or others, if that has increased? This was part of the International Center for Missing & Exploited Children's data.

Mr. ALLEN. Right. We——

Senator CANTWELL. And that was, one in five children ages 10 through 17 has been solicited online——

Mr. ALLEN. That——

Senator CANTWELL.—for unwanted sexual advances. So——

Mr. ALLEN. The one-in-five data were from Dr. Finkelhor's research, which the University of New Hampshire conducted for the National Center in 2000. The good news is, his most recent version of that indicated that that number has gotten a little better. It's now one in seven.

In terms of child pornography cases, we don't have the same kind of scientific data. What I can report to you is that the numbers of child pornography reports received by the National Center for Missing & Exploited Children are up dramatically.

The other thing that we're seeing from those reports is that the victims are getting younger. Again, citing Dr. Finkelhor's research from a couple of years ago looking at offenders, what we've found is that most people don't understand what the true composition of this issue is. His research found that 39 percent of the offenders who were identified had images of children younger than 6 years old; 19 percent, younger than 3. Many people think this is a problem of 20-year-olds in pigtails made to look like they're 15. It's not. Overwhelmingly, the demand is for prepubescent children, and the numbers are getting younger and younger.

Senator CANTWELL. So, if you were going to say the decrease of—in fact, if it is a decrease—and, you know, you never know what's going on; it may be that people have gotten better at hiding the contacts or who knows, maybe software on the other side, and encryption technology, who knows what's happening. But, let's say, for example—for sure there is an improvement in the situation. To what do we think we can attribute the effort that led to that reduction?

Dr. FINKELHOR. One of the things that we found was that young people, between 2000 and 2005, when we did our two surveys, reported they were going to chat rooms less, that they were talking to people that they don't know less, and it suggested that actually they had gotten some of the prevention education messages that we had been putting out, and that was the good news.

I don't want to put too much stock in the decline from the one in five to the one in seven. We didn't see a change in the number of kids who were experiencing what we call "aggressive solicitations." Those were the really endangering ones, where the person who was soliciting them tried to make contact with them offline,

in addition to the computer communication. That stayed at around 4 percent. Those are the ones that concern me, that one in 20. Most of the kids are handling those pretty well, the other ones, that don't involve these aggressive solicitations. Unfortunately, the aggressive solicitations did not decline.

Senator CANTWELL. And, Mr. Allen, I'm assuming that the National Center does work with the International Center on——

Mr. ALLEN. Yes.

Senator CANTWELL.—on these efforts, since the Internet is global and——

Mr. ALLEN. Absolutely.

Senator CANTWELL.—and so, that connectivity issue and data storage issue is being addressed on an international basis, because you don't want to just chase the problem to some server somewhere else that isn't regulated. So, are we working on that, on an international basis?

Mr. ALLEN. Senator Cantwell, we're working on it. In fact, you helped us launch our partnership with Interpol on that. The great challenge, internationally, is that we reviewed the law in the 186 member countries of Interpol, and we found that 95 of them have no law at all, child pornography is not even a crime. And in 136 of the member countries of Interpol, the possession of child pornography is not a crime. It is a real challenge, because, in much of the world—this is now an issue in which Eastern European organized crime is very much involved, because it's so easy and so profitable. And we have great work we need to do work to change the law around the world and build capacity. With Interpol, we've now trained law enforcement in 100 countries to build capacity——

Senator CANTWELL. And do——

Mr. ALLEN.—but there's a long way——

Senator CANTWELL. And do you have——

Mr. ALLEN.—to go.

Senator CANTWELL. And do you have data from that, Mr. Allen, about the success of that? Do you have any statistics from that?

Mr. ALLEN. From the legislative research?

Senator CANTWELL. No, from that 2004 Interpol effort of training law enforcement to identify an online crime scene, so they could better find the perpetrators. That training, which I did applaud, I thought was a useful effort, particularly given, again, that so much of these activities, from an international basis, are going to impact us here in the United States. We can do a really good job of trying to clean things up here, but, if we're seeing Websites, you know, from all over the globe——

Mr. ALLEN. Absolutely. We——

Senator CANTWELL. So——

Mr. ALLEN.—can certainly get you the data that was generated.

Senator CANTWELL. So, do you think that that's worked, this—here's my point. I think everybody's doing great work, but we definitely have an enormous task in front of us, and we're only going to have increases in communication and technology. We do want to use that to our advantage. But, measuring what—to the best of our degree—what is being successful, so that we can invest more in it, I think, is critical, at this early stage.

Mr. ALLEN. I agree. And there's very little research, or very little empirical data, on this issue outside the United States, and that's a real challenge.

Dr. FINKELHOR. And even the information that we have within the United States, I'm afraid, is woefully inadequate, in many respects, for tracking what's going on. I would just contrast the information that we have on infectious diseases, for example, which are another threat to the public, but we have tremendous information about infectious agents and accidents that we can track, over time, to see how we're doing. In the crimes-against-children area, we are woefully lacking, with just general epidemiological information, on some of the things that are most frightening to families, like abductions and Internet crimes against kids, and we could really improve. And it would answer some of the questions that you're interested in, I think.

Senator CANTWELL. Well, I think it's very important.

Again, Mr. Chairman, thank you for the hearing, and thank everybody on the panel for your hard work. But we obviously have a lot more work to do.

Thank you.

The CHAIRMAN. Thank you very much.

I've been listening intently to the testimony. And, according to reports that we have gathered, about 5 years ago there were about 100,000 child pornography Websites. Today, I think they get close to 400,000. At the same time, over 70 percent of children, teenagers, preteenagers, have viewed child pornography on the Internet. At the same time, we have statistics that suggest that the American family, 67 percent have both parents living with their children, the remainder are either living in homes, institutions, or with single parents, or with grandparents. At the same time, statistics suggest to us that most of these single parents are so overwhelmed with trying to make a living, they spend very little time with their kids. And I believe in parental involvement, but these numbers suggest that, for many of our kids, parental involvement does not exist. And so, I am concerned about what the Federal District Court in Utah did—making one of those laws unconstitutional. What I'd like to know is, What can we do—and maybe this is in the jurisdiction of the Judiciary Committee—to toughen the laws?

Now, for the record, what are the punishments that we have in the books, at this time?

Mr. ALLEN. Well, Senator, the Congress, certainly on Federal offenses, over the past several years has increased penalties significantly. And I think that's been a huge step forward. The States have some more work to do.

On the issue you raised about the Utah court decision, my reaction certainly is one of discouragement. This Congress has tried very hard to address this issue with governmental solutions, limiting the access, filtering and blocking and keeping kids from reaching this kind of content, or content reaching them.

Frankly, I think my judgment is that one of the things this Commerce Committee can do is to encourage and promote more private-sector innovation, because there are tools that are being developed. Ms. Jones talked about some of the leadership within the technology industry. I think there are tools that are being developed on

the private side that should be encouraged, should be examined, and we should begin to try to implement them.

Frankly, the courts have sent a pretty loud-and-clear message, and that message is, they're going to look very carefully at governmental regulatory mandates in some of the areas. And I think what the Congress has to do is look for a balanced approach, not that previous approaches weren't—but a more balanced approach that put greater emphasis on private-sector tools and private-sector innovation.

The CHAIRMAN. How can we convince our parents that what is involved here is serious, dangerous, and will just eventually break up families? What can we do? Can we do anything, legislatively?

Mr. ALLEN. Well, Mr. Chairman, our view, from the beginning, has been that this is a three-pronged process. One, the kind of activity we're talking about, almost without exception, is illegal. And so, I think law enforcement—an increased emphasis on law enforcement to identify those who are misusing the Internet for unlawful purposes, is more important than ever before.

Second, I think we have to continue the drumbeat to try to motivate America's parents, and awaken them. We live in a unique time, in which kids know more about a transcendent technology in our lives than do their parents. There are some terrific models and programs out here. Jackie Leavitt, the wife of the HHS Secretary, is here with us this morning. She has mobilized the Nation's first ladies around a program called iKeep Safe. There is a terrific training program that's gone into schools across the country, called i-SAFE. We, at the National Center, created, with Boys and Girls Clubs of America, an interactive online educational tool, called NetSmartz, with animation for younger kids. There are great tools out there. The Virginia model of mainstreaming it, of institutionalizing it, for making it a part of ongoing educational curricula, I think, is real important. So, we have to continue to emphasize and promote prevention and education.

But, third, I think the ultimate answer to a lot of this problem, frankly, is rooted in technology. The softwares have not yet been developed that can automatically identify, interdict, prevent certain kinds of issues. Members of this Committee talked, this morning, about the concern about a hands-off approach. I think if we continue to promote technology innovation to develop tools that can be used to prevent the most heinous of these problems, while emphasizing education in the classroom as an ongoing and integral part of what kids are taught and what they learn, continue the efforts to reach out to parents, recognize it's hard, but we've got to do it, and then give law enforcement the tools and the resources they need to go after, and prosecute, the "bad guys". The good news is, there have been thousands of them brought to justice. The bad news is, there are far more of them than we thought there were. And the reality is, as someone raised earlier, the Internet does create a situation where people can be anonymous, they can fantasize in the privacy of their own homes, they have little risk of detection. That's something we have to deal with.

The CHAIRMAN. Any closing remarks here?

Miss America?

Ms. NELSON. Again, thank you for the opportunity for allowing me to be here to speak on this issue. I feel that the legislation has been put in place, that there are things being done that are the step in the right direction, but there is more that we can do. Again, I want to promote education, because I feel that education on this issue will help to keep our kids, and help them from being the victims in the first place. If we can police the Internet on our side of the keyboard, I think that's the best way to go about this issue.

The CHAIRMAN. Thank you.

Dr. Finkelhor?

Dr. FINKELHOR. I want to thank you, also, for the opportunity to address the Committee, and also appreciate your interest in this topic.

My final remark is that the vulnerability of children on the Internet is an extension of their vulnerability in every aspect of their lives, and we should not ignore that, as well, as we try to face the risks that are posed online. But children are still being bullied in school, sexually abused in their families, and they are still witnessing domestic violence in their homes. And this is all part of one fabric and in order to address victimization online, we also need to address some of these other issues, as well.

The CHAIRMAN. Mr. Allen?

Mr. ALLEN. Just, finally, Mr. Chairman, thank you for the opportunity, and thank you for your extraordinary leadership and commitment on this issue. This is timely, and it's important.

The CHAIRMAN. Mr. Neugent?

Mr. NEUGENT. Thank you, Mr. Chairman, also, for allowing me to speak today. I do believe that education is one of the answers, and we will continue to pursue that in Virginia. We will continue to work with the attorney general's task force. And we hope, at some point, to have information to show that, in effect, our programs are working.

Thank you very much.

The CHAIRMAN. Ms. Jones?

Ms. JONES. Thank you, Mr. Chairman.

I'm sure you know, but your staff, James Assey and Margaret Cummisky and the people that work behind you, are tirelessly pursuing this, that the staff members of every Committee member here that we've met with who pursue this issue are. We are profoundly grateful for that, because, we feel like we're out on the front line, trying to defend this thing. It's nice to know that somebody in Washington is paying attention to it.

It seems like a noncontroversial issue, nonpartisan. Nobody thinks child predators are a good idea. So, we would continue to urge passage of the McCain-Schumer child pornography bill, the bill that Senator Pryor mentioned, in regards to online parental controls. Any of the tools that are small steps in the overall solution, we would encourage this Committee to continue to pursue.

But, most importantly, just thank you so much for taking a look at the issue and for making it a priority at the end of a session and on a hot summer day, when you might be off doing something else. So, we are just profoundly grateful for that.

Thank you.

The CHAIRMAN. Obviously, there's much to be done. And we're not quite knowledgeable as to what should be done.

But, Mr. Allen, we will find out. And I promise all of you that we'll make it tougher, we'll get more parents involved, we'll have PTAs involved. And that has been a concern of mine. I used to attend PTA meetings, as a Member of Congress, which meant I had to miss some votes. But, today, in a school of, say, 500 children, if you have 50 parents at a PTA meeting, you are doing very well, which is sad. It wasn't so in my days of youth. But I suppose, with all the advancement and technology advancements, we don't need these things. But I think they're wrong. Parents must get involved.

And I thank you all very much for your contribution.

The session is adjourned.

[Whereupon, at 11:52 a.m., the hearing was adjourned.]

○