H.R. 5319, THE DELETING ONLINE PREDATORS ACT OF 2006

HEARING

BEFORE THE

SUBCOMMITTEE ON TELECOMMUNICATIONS
AND THE INTERNET

OF THE

COMMITTEE ON ENERGY AND
COMMERCE
HOUSE OF REPRESENTATIVES

ONE HUNDRED NINTH CONGRESS

SECOND SESSION

JULY 11, 2006

Serial No. 109-121

Printed for the use of the Committee on Energy and Commerce

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

U.S. GOVERNMENT PRINTING OFFICE

30-410PDF WASHINGTON : 2006

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

COMMITTEE ON ENERGY AND COMMERCE

JOE BARTON, Texas, *Chairman*

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

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

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

SUBCOMMITTEE ON TELECOMMUNICATIONS AND THE INTERNET

FRED UPTON, Michigan, *Chairman*

MICHAEL BILIRAKIS, Florida
CLIFF STEARNS, Florida
PAUL E. GILLMOR, Ohio
ED WHITFIELD, Kentucky
BARBARA CUBIN, Wyoming
JOHN SHIMKUS, Illinois
HEATHER WILSON, New Mexico
CHARLES W. "CHIP" PICKERING, Mississippi
VITO FOSSELLA, New York
GEORGE RADANOVICH, California
CHARLES F. BASS, New Hampshire
GREG WALDEN, Oregon
LEE TERRY, Nebraska
MIKE FERGUSON, New Jersey
JOHN SULLIVAN, Oklahoma
MARSHA BLACKBURN, Tennessee
JOE BARTON, Texas
(EX OFFICIO)

EDWARD J. MARKEY, Massachusetts
Ranking Member
ELIOT L. ENGEL, New York
ALBERT R. WYNN, Maryland
MIKE DOYLE, Pennsylvania
CHARLES A. GONZALEZ, Texas
JAY INSLEE, Washington
RICK BOUCHER, Virginia
EDOLPHUS TOWNS, New York
FRANK PALLONE, JR., New Jersey
SHERROD BROWN, Ohio
BART GORDON, Tennessee
BOBBY L. RUSH, Illinois
ANNA G. ESHOO, California
BART STUPAK, Michigan
JOHN D. DINGELL, Michigan
(EX OFFICIO)

CONTENTS

Page

Testimony of:

Abbott, Hon. Greg, Attorney General, Office of the Attorney General, State of Texas ... 25

Aftab, Esq., Parry, Executive Director, WiredSafety.org ... 31

Collins, Michelle, Director, Exploited Child Unit, National Center for Missing and Exploited Children ... 90

Davis, Ted, Director, Knowledge Asset Management, IT Department, Fairfax County Public Schools ... 95

Kelly, Chris, Vice President, Corporate Development and Chief Privacy Officer, Facebook ... 104

Lenhart, Amanda, Senior Research Specialist, Pew Internet and American Life Project . 111

Yoke, Beth, Executive Director, ALA Young Adult Library Services Association ... 127

Zellis, David W., First Assistant District Attorney, Office of the Bucks County District Attorney, Commonwealth of Pennsylvania ... 135

Additional material submitted for the record:

Racine, Elizabeht, prepared statement of ... 154

Resnick, Michael A., Associate Executive Director, National School Boards Association, prepared statement of ... 158

H.R. 5319, THE DELETING ONLINE PREDATORS ACT OF 2006

TUESDAY, JULY 11, 2006

HOUSE OF REPRESENTATIVES,
COMMITTEE ON ENERGY AND COMMERCE,
SUBCOMMITTEE ON TELECOMMUNICATIONS AND THE INTERNET,
Washington, DC.

The subcommittee met, pursuant to notice, at 10:10 a.m., in Room 2123 of the Rayburn House Office Building, Hon. Fred Upton [Chairman] presiding.

Members present: Representatives Upton, Gillmor, Whitfield, Cubin, Shimkus, Wilson, Bass, Walden, Terry, Ferguson, Blackburn, Barton [ex officio], Markey, Engel, Wynn, Gonzalez, Inslee, Eshoo, and Stupak.

Also Present: Representatives Fitzpatrick and Kirk.

Staff Present: Howard Waltzman, Chief Counsel for Telecommunications and Internet; Anh Nguyen, Legislative Clerk; Jaylyn Jensen, Senior Legislative Analyst; Johanna Shelton, Minority Counsel; and David Vogel, Minority Research Assistant.

MR. UPTON. Morning, everyone. Today we are holding a hearing on H.R. 5319, the Deleting Online Predators Act of 2006, which was introduced recently by Representatives Fitzpatrick and Kirk.

Under the leadership of Chairman Whitfield and Chairman Barton, the Oversight and Investigations Subcommittee has held multiple hearings, exposing the appalling sexual exploitation of children on the Internet. This includes the dark underside of social networking websites, which have become stalking grounds for sexual predators who are preying on children all across the Nation. We have had many such cases in my own State of Michigan, far too many.

Federal law enforcement officials have described the sexual abuse and exploitation of our Nation's youth as an "epidemic" propagated by the unlimited access of the Internet. The statistics are alarming. The FBI has seen a 2,026 percent increase in its caseload of online sexual predators in the last 10 years. Of the estimated 24 million child Internet users, one in five kids has received unwanted sexual solicitations. It is estimated that at any given moment, 50,000 predators are prowling for children online, many of whom are lurking within social networks.

At a minimum, what our hearings have taught us is that both children and parents need to become better educated about the dangers of social networking websites, and parents need to police their children's online use at home to guard against sexual predators.

However, to the extent that children are using the Internet outside the home, particularly at school or at the public library, parents are not able to monitor their children's online use, and that is a situation that H.R. 5319 is designed to address.

At its heart, H.R. 5319 would require schools and libraries which receive E-rate funding to restrict minors' access to commercial social networking websites through which such minors may easily be subject to unlawful sexual advances, unlawful requests for sexual favors, or repeated offensive comments of a sexual nature from adults.

The approach taken by H.R. 5319 is not dissimilar to the approach taken by the Children's Internet Protection Act, through which Congress requires schools and libraries that receive E-rate funding to impose filtering technology to protect kids from online visual depictions of an inappropriate sexual nature.

I have long supported and remain a strong supporter of the E-rate. I visit a school every week and I have seen the tremendous educational value which the Internet has brought to students throughout my congressional district, and I recognize the importance of the E-rate in making this a reality.

However, as with all technologies, the Internet is a double-edged sword, and Congress has a responsibility to ensure that, to the extent that a Federal program is involved, it is doing all that it can to ensure that kids are protected from online dangers.

H.R. 5319 represents yet another step in making our children's online experience at school or at the library safe. I want to thank our witnesses for being with us today, and I look forward to hearing their views on H.R. 5319, and I yield to the gentlelady from California for an opening statement.

[Prepared statement of Hon. Fred Upton follows:]

PREPARED STATEMENT OF THE HON. FRED UPTON, CHAIRMAN, SUBCOMMITTEE ON TELECOMMUNICATIONS AND THE INTERNET

Good morning. Today we are holding a legislative hearing on H.R. 5319, the "Deleting Online Predators Act of 2006," which was introduced by Representatives Fitzpatrick and Kirk.

Under the leadership of Chairman Whitfield and Chairman Barton, the Oversight and Investigation Subcommittee has held multiple hearings exposing the appalling sexual exploitation of children on the internet. This includes the dark underside of social networking websites, which have become stalking grounds for sexual predators who are preying on children all across the nation. We have had many such cases in my own home state of Michigan…far too many.

Federal law enforcement officials have described the sexual abuse and exploitation of our nation's youth as an "epidemic" propagated by the unlimited access of the Internet.

The statistics are alarming - the FBI has seen a 2,026% increase in its caseload of online sex predators in the last 10 years. Of the estimated 24 million child Internet users, one in five kids has received unwanted sexual solicitations. It is estimated that at any given moment, 50,000 predators are prowling for children online – many of whom are lurking within social networks.

At a minimum, what our hearings have taught us is that both children and parents need to become better educated about the dangers of social networking websites, and parents need to police their children's on-line use at home to guard against sexual predators.

However, to the extent that children are using the Internet outside the home, particularly at school or at the public library, parents are not able to monitor their children's on-line use – and this is the situation that H.R. 5319 is designed to address.

At its heart, H.R. 5319 would require schools and libraries which receive e-rate funding to restrict minors' access to commercial social networking websites through which such minors may easily be subject to unlawful sexual advances, unlawful requests for sexual favors or repeated offensive comments of a sexual nature from adults.

The approach taken by H.R. 5319 is not dissimilar to the approach taken by the Children's Internet Protection Act, through which Congress requires schools and libraries that receive e-rate funding to impose filtering technology to protect kids from on-line visual depictions of an inappropriate sexual nature.

I have long supported the e-rate, and I continue to do so. I visit a school a week and have seen the tremendous educational value which the Internet has brought to students throughout my district, and I recognize the importance of the e-rate in making this a reality.

However, as with all technologies, the Internet is a double-edged sword, and Congress has a responsibility to ensure that, to the extent that a federal program is involved, it is doing all that it can to ensure that children are protected from on-line dangers. H.R. 5319 represents yet another step in making our children's on-line experience at school or at the library safe.

So, I want to thank our witnesses for being with us today, and I look forward to hearing their views on H.R. 5319.

MS. ESHOO. Thank you, Mr. Chairman. And thank you to all of the witnesses that are here today. We are going to learn from you. I would particularly like to welcome Chris Kelly, who is representing Facebook, a company that is located in the heart of my congressional district, Palo Alto. So thank you for traveling across the country and being here with us today.

Without a doubt, everyone here today, everyone, whether they are at the witness table, in the audience in the hearing room, and the Members of Congress that are here, are concerned about predators that stalk the most vulnerable in our society, our children. I think the most important thing that can come out of the hearing today is raising the awareness of the problem and what some of the solutions are.

Certainly the bill directs itself to be a solution. I think we need to build on that. This is an issue that parents--I don't think we need to teach them more about it. They are already concerned. They want solutions; that is our job.

I think it is important for us to all understand that the computer that is in our den or in the family room or in our children's bedrooms is really a public space, and I don't think we think of it that way. A computer with Internet access is no more private than a busy street or the mall or the grocery store unless we take steps to secure it. No parent or teacher would drop a child off in Times Square and say, "Have fun, make sure you don't leave the Disney store." That just isn't a reality. So why would anyone turn their children loose on the Net without supervision and other safeguards to protect them?

Nothing is more important than close supervision, and monitoring of a child's Web surfing, and a host of tools are available to make this difficult task even easier and more effective.

Ten years ago, I introduced legislation, the On-Line Parental Control Act, to encourage the use of technology, and most Internet service providers now offer parental control tools to their customers. Combined with technological support, parental vigilance is the single most effective thing anyone can do to stop online predators. I believe that, and I think it has been borne out.

I think we also have to bear in mind that the Internet and many of the sites we will be discussing today are the source of great convenience, enriching our educational experiences, and collectively are the leading sector of our economy. Just as the Net has revolutionized communications, e-mail, instant messaging, VOIP, and e-commerce, websites like Friendster, MySpace, and Facebook have transformed the way we, particularly young people, socialize, make new friends, and establish business contacts. These are tremendous new services, and Web networking is by no means a negative development, but it does create real challenges for companies, for policymakers, and for parents to ensure the safety and well-being of our kids.

We have to confront these challenges in a way that addresses the dangers that exist, without causing unnecessary collateral damage to some of the very valuable sites and services now available on the Net. And I think that this is going to be a real valuable exercise in terms of this hearing because the working knowledge of Members that are going to make these policy decisions, in my view, needs to be broadened and deepened at the same time.

So I look forward to hearing from each one of the witnesses. Mr. Chairman, thank you for your able leadership of our subcommittee, and thank you for having this hearing today.

MR. UPTON. I thank the gentlelady. I would ask at this point unanimous consent that the two sponsors of the bill, Mr. Kirk and Mr. Fitzpatrick, might be able to participate in the hearing and, obviously, follow the regular order, which would be after the members of the subcommittee. And without hearing objection, that should be the case.

We would recognize for an opening statement the Chairman of the full committee, the good gentleman from Texas, Mr. Barton.

CHAIRMAN BARTON. Thank you Mr. Chairman. I want to extend a personal welcome to my good friend, personal friend of longstanding, Attorney General of Texas, Greg Abbott. Glad to have you here, General. We appreciate you being willing to testify on this small panel of seven other people. We appreciate your humility, and we certainly appreciate your service to the State of Texas and extension of some of the things you are doing for the citizens of our entire country.

We are here today to have a legislative hearing on H.R. 5319, the Deleting Online Predators Act of 2006. It has been authored by Congressman Fitzpatrick, who is also with us up here on the dais. I would like to welcome some of our witnesses who have testified before Mr. Whitfield's subcommittee, who has been holding a hearing on this malaise. We have Mr. Chris Kelly from Facebook, we have Parry Aftab from WiredSafety.org. They have already participated in Mr. Whitfield's hearings, and we are glad to have you here at the legislative hearing.

We were not able to get a representative of MySpace to testify at today's hearing, which I think is unfortunate. The Oversight and Investigations Subcommittee has been holding a series of hearings to investigate the sexual exploitation of children on the Internet. The hearings have focused on the growing Internet child pornography trade, and the tools that sexual predators use to victimize our children. We have also tried to determine what, if anything, is being done or can be done to find, prosecute, and convict the child predators in our society.

The Oversight Subcommittee has heard from the Federal Trade Commission, Federal Communication Commission, law enforcement agencies, children subjected to sexual abuse, victims' advocates, and some of these Internet service providers.

H.R. 5319 targets children's use of social networking websites and chat rooms in schools and libraries. As participation in these Internet "social communities" rises to record numbers, so do the news reports of a multitude of potential dangers they pose.

There is no question that the Internet does and will continue to provide innovative benefits to society. However, we must take steps now to protect our children, and this is a priority of this subcommittee and also of the full committee, and, I might add, it is a priority on both sides of the aisle. Mr. Dingell shares this concern just as much as I do. We need to prevent predators from using the Internet and social networking sites, in particular to prey on our children.

I look forward to hearing from our witnesses today in order to better understand the social networking phenomenon, the benefits and the problems that it creates. If we can understand this, it will enable us to strike the right balance regarding the appropriate role for the Federal government and Federal legislation to play in helping our educators keep our children safe on the Internet.

It would seem to me that H.R. 5319 is a step in the right direction. Schools and libraries that receive universal service subsidies have an obligation to ensure that their subsidized communication services do not become a hunting ground for pedophiles. If social networking sites are not taking the necessary precautions to prevent the exploitation of children, then, at the very least, Congress should prohibit the use of federally mandated funds to access Internet sites that put children in harm's way.

Again, I want to thank Attorney General Abbott for being here. I want to thank the other witnesses for being here. And I thank you, Mr. Chairman, for holding this hearing.

[Prepared statement of Hon. Joe Barton follows:]

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

Mr. Chairman, thank you for holding this hearing today on H.R. 5319, the "Deleting On-line Predators Act of 2006" authored by Congressman Fitzpatrick. I'd like to once again welcome Mr. Chris Kelly from Facebook, and Ms. Parry Aftab from WebSafety.org, both of whom have participated in earlier hearings held by our Oversight and Investigations Subcommittee, on the issue of sexual exploitation of children over the Internet. Although I am disappointed that Myspace declined to send a representative to attend today's hearing, I would like to offer a warm welcome to the Attorney General from my home state of Texas, The Honorable Greg Abbott. Thank you - and all of the witness on the panel - for taking the time out of your busy schedules to appear before us today.

The Oversight and Investigations Subcommittee is currently holding a series of hearings to investigate the sexual exploitation of children on the Internet. The hearings have focused primarily on the growing Internet child pornography trade, the tools sexual predators use to victimize children, and what can, and is, being done to find, prosecute and convict child predators. The Subcommittee has heard from the FTC, FCC, law enforcement agencies, children subjected to abuse, victims advocates, and most recently from Internet Service Providers and social networking site owners.

H.R. 5319 targets children's use of social networking websites and chat rooms in schools and libraries. As participation in these Internet "social communities" rises daily in record numbers, so do the news reports of a multitude of potential dangers they pose.

There is no question that the Internet does and will continue to provide innovative benefits to society far into the future. However, the protection of our children must be a priority of this government and of our society. We need to prevent predators from using the Internet, and social networking sites in particular, to prey on children.

I look forward to hearing from our witnesses today in order to better understand the social networking phenomenon and the benefits and problems it creates. Understanding this will enable us to strike the right balance regarding what role, if any, the Federal Government and educators should play in keeping our children safe on the Internet.

H.R. 5319 is certainly a step in the right direction. Schools and libraries that receive universal service subsidies have an obligation to ensure that their subsidized communications services do not become a hunting ground for pedophiles. If social networking sites are not taking the necessary precautions to prevent the exploitation of children on their sites, then, at the very least, Congress should prohibit the use of federally-mandated funds to access Internet sites that put children in harm's way.

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

MR. UPTON. At this point I would recognize the gentleman from Texas, Mr. Gonzalez.

MR. GONZALEZ. I commend you for all of your efforts, and I want to welcome all of the witnesses but, again, I want to echo the sentiments of the full committee, Mr. Barton, in welcoming our esteemed Attorney General Greg Abbott who served admirably on our Supreme Court. It is good to see you again. As we speak, there are different maps being drawn regarding our congressional districts. So I really do welcome you, Greg.

But, seriously, what we are dealing with today cannot be adequately emphasized as to the importance of our respective constituencies. This is something that is commonly held no matter where you go, whether it is a Republican or a Democratic district, regardless of the region and such. The question really is: What can we do in a practical sense and technologically that is feasible, and looking at the legalities too?

So I really do welcome Greg's perspective on this. But overall, at the end of the whole process, this is really quite limited when you think in terms of libraries, schools, and so on. And the legal nexus that allows us to provide or mandate certain conditions on these institutions and such is really the Universal Service Fund; and that is another issue, by the way, which has still not been resolved by this committee as we move forward regarding that particular issue.

So it is important to keep that in mind. In other words, what gives this Congress jurisdiction to impose those particular conditions? At the end of the process, though, we have to see what is the potential of the unintended consequence of the legitimate use of the Internet, and I think this committee is always driven with that particular goal in mind. And it is what we are doing because we know there are always going to be criminal and illegitimate uses of the Internet, but as we attempt to govern those and address the concerns of our constituents, the big picture, though, is the majority of the use of the Internet is legitimate, and it has been a tremendous economic accelerator and such for this country, and we can't again impede its progress. But nevertheless, I think that we can still have the best of both worlds, and hopefully the testimony of the witnesses will guide us there today, and I yield back.

Thank you, Mr. Chairman.

MR. UPTON. Mr. Gillmor.

MR. GILLMOR. Thank you very much, Mr. Chairman, and I appreciate your holding this hearing. As a member of both this subcommittee and as a strong advocate of strong sex offender laws, I think this hearing is an important step in protecting our children from violent predators. As a sponsor of two bills, H.R. 95 and H.R. 4815, which were aimed at giving American families access to necessary information they need to protect themselves from violent sexual offenders through a national database. I point out that both of those bills have been incorporated in other legislation and have now passed the House of Representatives. However, I believe that our schools and our libraries have been taken for granted as a safe haven that is free of illicit and illegal cyber content. Unfortunately, we know that is not the case. And I agree with the concepts promoted by H.R. 5319--but I believe that today's discussion is simply the beginning of an in-depth dialogue between policymakers and industry leaders. Clearly, social networking and chat technologies are not inherently bad and they offer many benefits. Yet, in using them, we have to be sure that we protect the safety of our children.

A recent study funded by the National Center For Missing and Exploited Children, Dr. David Finkelhor, Director of Crimes Against Children Research Center, found that one out of every five children received a sexual approach or a solicitation over the Internet in the past year. Additionally, in a separate study commissioned by the National Association of School Resource Officers and conducted by the National School Safety and Security Services, the leading independent national school safety and security firm based in Cleveland, Ohio, showed 55 percent of school safety officers stating that concerns regarding Internet-based crimes had increased in their school community in the past 2 years. These are alarming statistics and I think we ought to take the necessary steps to protect our Nation's families before tragedy can befall other witnesses.

Mr. Chairman, I have been pleased to work closely with the Safe Now Project on the two bills of mine that I mentioned, and I look forward to working with them, members of this committee, industry, and leadership to ensure that our Nation's children are protected, while allowing consumers to continue to realize the benefits of these technologies. And I yield back.

[Prepared statement of Hon. Paul E. Gillmor follows:]

PREPARED STATEMENT OF THE HON. PAUL E. GILLMOR, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF OHIO

Thank you for holding this very important hearing. As a member of this subcommittee and as a strong advocate for increasing our nation's sex offender laws, I see this hearing as an important step in protecting our country's children from violent predators.

As the sponsor of two bills, H.R. 95 and H.R. 4815, aimed at giving American families unfettered access to the necessary information they need to protect themselves from violent sexual offenders, I believe that our schools and libraries have been taken for granted as a safe haven that is free from illicit and illegal cyber content. Although I agree with the concepts promoted by H.R. 5319, I believe today's discussion is simply the beginning of an in-depth dialogue between policymakers and industry leaders because social-networking and chat technologies are not inherently bad and offer many benefits—yet we must ensure the safety of our children.

In a recent study funded by the National Center for Missing and Exploited Children, Dr. David Finkelhor, Director of the Crimes Against Children Research Center, found that one in every five children received a sexual approach or solicitation over the Internet in the past year. Additionally, in a separate study commissioned by the National Association of School Resource Officers and conducted by National School Safety and Security Services, a leading independent national school safety and security firm based in Cleveland, Ohio, showed 55% school safety officers stating that concerns regarding Internet-based crimes had increased in their school-community in the past two years. Mr. Chairman, these are alarming statistics and we must take the necessary steps to protect our nation's families and before tragedy can befall another needless victim.

Mr. Chairman, I have been pleased to work closely with the Safe Now Project on both of my bills, and I look forward to continuing to work with them, members of this committee, industry, and leadership to ensure that our nation's most precious assest—our children—are protected while allowing consumers to continue to realize the benefits of these technologies. This challenge must be met and a delicate balance must be struck, but we must come together in good faith to make certain that our schools and libraries continue to be a sanctuary for learning and growth.

MR. UPTON. I thank the gentleman, and recognize the Ranking Member of the subcommittee, Mr. Markey from Massachusetts.

MR. MARKEY. Thank you, Mr. Chairman, very much. And I want to commend you, Mr. Chairman, for calling this hearing this morning on Internet chat rooms and social networking sites and legislation making certain requirements on K through 12 schools and libraries seeking to receive E-rate funding. There is a rising concern over Internet sites in the context of child exploitation. The Oversight and Investigations Subcommittee has held several hearings on this subject. While there are age and other restrictions on many of the sites, including MySpace.com and Facebook, there are questions as to how such restrictions are verified and enforced. This subcommittee has a long history of working to ensure a safe environment for children on the Internet.

In 2000, Congress enacted the Internet safety requirements for schools and libraries receiving E-rate funding to ensure that such entities were monitoring children's online activities, to thwart access to material that was harmful to minors.

In addition, I cosponsored legislation with Representative John Shimkus, which promoted healthy and safe Internet surfing for children with the dot-kids law. That law establishes a domain for sites with content safe for kids and prevents any links outside of the domain.

Legislation before this subcommittee seeks to go further and proposes to create additional requirements on schools and libraries. These requirements would require K through 12 schools and libraries to certify that they prohibit access to social networking sites and chat rooms through which minors may easily access or be presented with indecent materials or easily be subjected to unlawful sexual advances. Without question, combating child exploitation and safeguarding children is a high priority.

In pursuit of that goal, we should be mindful, however, of devising new requirements that may be plagued by terminological inexactitude, a standard that is based upon what may or may not be easily accessed may be difficult to define and enforce.

In addition, I have reservations about utilizing the E-rate funding mechanism as the legislative hook for Federal involvement in this area. That is because the E-rate program was not designed to be a cop on the beat in the front lines, battling child predators. Rather, it was designed to enhance Internet access and bridge the digital divide. As a result, it is a program which may not help or assist all K through 12 schools at any time, or individual schools in every funding cycle.

In other words, if the goal is protecting children and combating child exploitation, why should these requirements only apply in schools receiving E-rate funding? In other words, only the poorest schools. Why should we not ensure that every child in every school be protected?

Our colleague, Representative Melissa Bean of Illinois, has similar legislation, the Safeguarding America's Families by Enhancing and Reorganizing New and Efficient Technologies Act of 2006, or the SAFER NET Act. This legislation puts authority in the Federal Trade Commission to establish an Office of Internet Safety and Public Awareness. That office would have the task of evaluating Internet safety efforts and activities provided at various levels of government, eliminating redundancy of efforts at various levels of government and serving as the primary contact in the Federal government, and as a national clearinghouse for information and public awareness efforts regarding Internet safety.

I commend that legislation as well to the subcommittee's attention, recognizing, Mr. Chairman, quite well, that it is not within our subcommittee's jurisdiction. However, it is within the full committee's jurisdiction, and it may warrant our attention as we continue to look into these matters.

I think it is important, Mr. Chairman, that we not be limited just to E-rate beneficiaries. I don't think that really should be the purpose of this legislation; otherwise, only if you are in a poorer school would you be protected. Whereas, we want to ensure that as we look at this issue, that there is, in fact, a universal application, or else in many ways it may be struck down as being unconstitutional, as not being a ubiquitous piece of legislation. So I yield back the balance of my time.

MR. UPTON. Mr. Shimkus.

MR. SHIMKUS. Mr. Chairman, I waive for questions.

MR. UPTON. Mrs. Wilson.

MRS. WILSON. Thank you, Mr. Chairman, and thank you for holding this hearing today. I wanted to also thank Congressman Fitzpatrick for his leadership on this issue. When kids are at a point in their lives where they are listening to their peers more than they are listening to their parents, it is at the point of which they are really most vulnerable, and that is really in the teen years where they are vulnerable to people who, if they met them in person, there might be more flags that went off that said there is something not right here, I don't like this, and they would be willing to walk away. But on the Internet, those flags that kids learn from a very young age about what is safe and what doesn't feel safe are often not there, or are intentionally hidden by people who want to exploit them.

It is very hard to raise G-rated kids in an R-rated world. And we should be able to give schools and parents more tools to allow their kids to grow up safely and to move towards being more independent, which is a very natural thing for teenagers while being still in a safe place.

My colleague, Mr. Shimkus, has led this effort on this committee on the dot-kids legislation, and Mr. Green of Texas and I sponsored legislation that ultimately became the CAN SPAM Act to allow parents to have control about the junk e-mail that comes into their homes, which has led to several prosecutions and a significant reduction in unsolicited commercial e-mail, particularly with pornographic content.

I think this legislation we are looking at here today will help schools battle a problem. In most middle schools, and certainly most high schools, kids can eat their lunch fast and go to the library to play games on the computers or use the Internet. Yet they are there, largely or loosely unsupervised. We need to make sure that that is a safe place for them to be.

I will also be interested in hearing from our panel, what other tools does law enforcement and industry need to track and prosecute predators, who are using places that may seem safe to kids, to prey on kids.

Thank you, Mr. Chairman, for this hearing, and I look forward to working on this legislation.

[Prepared statement of Hon. Heather Wilson follows:]

PREPARED STATEMENT OF THE HON. HEATHER WILSON, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF NEW MEXICO

Mr. Chairman, I thank you for holding this important hearing and compliment Congressman Fitzpatrick for his leadership on this issue.

Popular websites like *myspace.com*, *thefacebook.com*, *xanga.com*, and *friendster.com* have become the way teenagers communicate. When kids are at the point when their peers are starting to be more important than their parents, they are very vulnerable. Predators know this and are trolling the chat rooms pretending to be someone they are not.

Several of us on this committee have worked together to make the internet safer for children. It is hard to raise G-Rated children in an R-Rated world. In the 108th Congress, Mr. Green and I authored legislation that was enacted into law as part of the CAN-SPAM Act to give parents a way to control unsolicited email and put the electronic equivalent of a "brown paper wrapper" in the body of a message. We saw results with this piece of legislation with 4 people being indicted soon after the legislation was enacted and a dramatic reduction in spam – particularly pornographic spam.

In 2002 our colleague, Mr. Shimkus, authored the "Dot Kids Act" which passed the Congress and became law. The legislation created a second-level domain within the internet which promotes positive experiences for children and families using the internet and provides a safe online environment for children. Ultimately, it helps prevent children from being exposed to harmful material over the internet.

According to the Center for Missing and Exploited Children, more than 2,600 incidents have occurred where adults have used the internet to target children online in order to engage in sexual activity. Teenagers 13-18 often communicate over the internet with someone they have not met in person and 1/3 of those teenagers have talked about meeting someone they have only met through the internet.

The legislation we are considering today will help schools battle this problem by creating additional internet safety requirements for schools to receive universal service funding. Websites like *myspace.com* and the *facebook.com* do not belong in our schools. Parents need to be educated as to what these websites are and how their children's personal information can be made available by the click of a mouse. And law enforcement may need more tools to track these predators and prosecute them.

I look forward to the testimony today and how we can make the internet a safer place for children.

MR. UPTON. Mr. Inslee.

MR. INSLEE. Thank you. Having sat through the oversight hearings, I can tell you this makes the hair stand up on the back of your neck when you hear what is going on. And I do look forward to getting some legislation, but I have some concerns about this, though, both from not going far enough and also going too far.

Not going far enough, I do hope at some point the full committee will look at the issue of storage of records to help law enforcement. The one thing we have heard from law enforcement over and over again during oversight hearings, is the inability to track these offenders to get the information that needs to be retained so they can search them out and find them, is what we really need. That is the silver bullet for law enforcement. I hope at some point our full committee will do that. I don't think that is in this bill particularly.

Second, the bill doesn't really address the 99 percent of the communications where these take place, which is at home. And, finally, getting parents to have access to filtering software is where the real megatonnage is in this issue, and I hope at some point our committee will look at it.

Third, an overly broad aspect of it. This is a great utility and I think it is important when we talk about all the bad things happening on the Net; one of the reasons the kids are so much smarter than us is because they have access to the Internet. And you hate to shut it down. And, frankly, the way this bill is written, one of our concerns, it would essentially disable Web-based sites for schools. If you want to set up a school government on a website, you want to allow kids to vote for one another, to e-mail to one another, as I understand it this bill currently would shut that down. I don't think that is something we want to do. We do have prank calls, but we haven't outlawed the phone system. That is something we need to get to to outrefine this bill. Thank you.

MR. UPTON. Mr. Walden.

MR. WALDEN. Thank you, Mr. Chairman. I am going to waive my opening statement.

MR. UPTON. Mr. Terry.

MR. TERRY. I waive as well.

[Prepared statement of Hon. Lee Terry follows:]

PREPARED STATEMENT OF THE HON. LEE TERRY, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF NEBRASKA

Thank you Mr. Chairman Upton for holding today's hearing on how we can take action to protect our children from online predators.

My wife and I monitor my three young boys' internet activity at home closely. However, I'm appalled to think that my boys or other young children might be using taxpayer dollars and computers that are intended to be used for educational purposes to access social networking websites as MySpace.com, Facebook.com, or similar social networking websites that leave them vulnerable to online predators.

The focal point of today's hearing is primarily over the bill, HR 5319, the Deleting Predators Act of 2006. HR 5319 would require schools and libraries that receive Universal Service funds (E-Rate money) to enforce a policy that prohibits access to a commercial social networking website or chat room through which minors may access obscene material, or be solicited for offensive comments or actions.

I support this limited policing of the Internet because it is unacceptable that our students in public schools could be allowed to access harmful material. We would certainly not condone pornographic material being accessed in our schools and, after I visited MySpace.com I would say at best that some of the material on MySpace.com was highly suggestive and borderline offensive, if not in some cases clear pornography.

The fact that schools and libraries could lose Universal Service E-Rate money if violations occur does not bother me in the least. The intention of the E-Rate program is to ensure that our schools and libraries are connected so that every child has the potential to reach their capacity regardless of their location. Those goals are consistent with the over all Universal Service Fund and any attempt to permit this public system to be a conduit to a Commercial website should not be allowed.

HR 5319 is a step in the right direction to protect our minors from pedophiles that prey on our youth via the Internet. I look forward to hearing from today's witnesses and I hope that we move swiftly on legislation that will raise the profile on the dangers that the Internet can pose to our youth.

MR. UPTON. Mr. Ferguson.

MR. FERGUSON. Thank you, Mr. Chairman. Thank you for holding this hearing. I particularly appreciate Mr. Fitzpatrick's and Mr. Kirk's work on this issue, and I am certainly looking forward to hearing from our distinguished panel of witnesses today.

I particularly want to welcome Ms. Parry Aftab who is from New Jersey. She is the Executive Director of WiredSafety. She testified in our hearing yesterday, in our Oversight and Investigations Subcommittee field hearing in my district in New Jersey yesterday. She is familiar to members of this committee and she has done extraordinary work on this particular issue, and we are glad she is here.

As a member of the O and I Subcommittee of this committee, this is an issue that I have become very familiar with over the past several months, and it is probably the ugliest and most disturbing issue that I have seen in my years in Congress. We are all aware of the promises that the Internet holds for education, for socialization, for fun for our children. However, there is unfortunately a much darker side to the Internet that we all need to be very much aware of. This is the side of the Internet that poses hidden dangers for unsuspecting children who may think that they are just chatting with a friend a few States away or perhaps even in their own neighborhood.

In these hearings our subcommittee has heard from Internet service providers, from social networking sites, from law enforcement officials, and from young people themselves. All of these witnesses have done well in helping us to understand the problem of child exploitation over the Internet and what can be done to help protect our children from these predators who set out to harm them.

Just yesterday at the field hearing in my district in New Jersey, we heard testimony from an impressive group of witnesses, all with extensive experience in the field of child exploitation and Internet safety. They offered several suggestions not only to help our children stay safe while surfing the Net, but also in apprehending these people who prey on our children not only in their schools and in their friend's house, but even in the protection of their own bedrooms. Some of these suggestions included more Internet education and awareness for both children and their parents, extended data retention by Internet service providers to help law enforcement officials track these predators down, harsher penalties for sex offenders, and closer monitoring by parents of what their children are doing on the Internet.

I am pleased to be able to say that New Jersey has an exemplary law enforcement unit, dedicated to fighting cyber crime and apprehending child predators, and I am proud of our New Jersey law enforcement officers who told us their stories yesterday and who work tirelessly to put these offenders behind bars.

I also, of course, again want to commend the gentleman from Pennsylvania and the gentleman from Illinois for the work that they have done on this issue and for taking time from their schedules to testify at our--Mr. Fitzpatrick testified at our hearing yesterday--and for their attendance at our hearing today.

As our Energy and Commerce Committee moves forward with these hearings, we are all becoming acutely aware of the dangers facing our children on the Internet today. There has never been a greater need for us as lawmakers and, for many of us, as we can speak as parents, to take a stand to protect our children.

Again, thank you, Mr. Chairman, for holding this hearing and I look forward to hearing from our witnesses.

MR. UPTON. Mr. Stupak.

MR. STUPAK. Thank you, Mr. Chairman, for holding this important hearing on what Congress can do to delete online predators. As Ranking Member of the Oversight and Investigations Subcommittee I have been impressed, until recently, with the bipartisan and thorough nature of the subcommittee's continued work in this area. I am hopeful the O and I Subcommittee work will guide this committee as we draft legislation to best protect our children from online pornographers and child abusers.

We heard at the Oversight and Investigations Subcommittee hearings that ISPs have widely varied methods for blocking predators and pornography from their networks and records of reporting offenders to authorities. We must hold the ISPs, including social networking sites, accountable. As a result of the O and I Subcommittee's work, many ISPs have made or are planning substantial changes to their policies to protect our children.

While these recent actions are certainly welcome, they are not enough. The reporting requirements for ISPs need to be updated and enforced. This should be the primary focus of this committee. Furthermore, the committee should not ignore the testimony of the Federal Communications Commission and the Federal Trade

Commission, whose hands are tied by lack of authority and insufficient laws, respectively.

It is important to note, however, that during the series of O and I hearings, there is no mention of online child exploitation being specific problems at schools and libraries. Perhaps this is because there is already a law on the books that requires schools and libraries who receive E-rate support to monitor children's Internet use and to employ blocking technology from viewing obscene or harmful materials. Many schools and libraries already block sites such as MySpace.

While I support holding today's hearings to see if schools and libraries need to enact further safeguards, I believe the real threat lies in children using these sites in his or her own room without adult supervision.

The legislation before us today lacks many of the important reforms needed that came to light as a result of the O and I hearings and investigation. I commend the Chairman for holding today's hearing and starting down a path to craft comprehensive bipartisan legislation that responds to the concerns voiced by the experts, law enforcement, ISPs, and the victims themselves, and not to go off in a direction that will do nothing to really crack down on this problem.

So with that, Mr. Chairman, I will yield back the balance of my time.

MR. UPTON. Mrs. Blackburn.

MRS. BLACKBURN. Thank you, Mr. Chairman. I want to welcome our witnesses and thank you for the hearing today and also to thank Chairman Stearns. I am on the O and I committee and we have spent a lot of time holding hearings and working on this issue. We appreciate that many of you have been with us before, and we appreciate that you have returned to us today.

I do want to say that as we worked through these hearings and have addressed some of the issues, that we have seen some pretty encouraging signs from the industry and from some of those that have been involved in the issue. Fox Interactive Media, the parent company of MySpace, in some of the work that MySpace is doing, they are taking some steps that are focused on security and protections for our minors, those that are under 18, and they have also taken some initiatives to start working with law enforcement agencies to protect children and to rout out the child predators. And this is the kind of activity that we appreciate seeing, and the kind of partnerships that we are anxious to see, and we are anxious to monitor this progress.

And I would encourage all of you to remember, now is the time for innovative ideas and now is the time for thinking outside the box, and now is the time to participate with us as we move forward on this. This is a tragic, tragic issue, online sexual predators who are using computers and the Internet to enter the safe haven of the home and attack these children.

So your presence and your work, the diligence of our Chairman and our committees and our staff, who has been so committed as we work through this, we do appreciate. I know there are lots of concerns with the bill that is before us, but I do want to thank Mr. Fitzpatrick and Mr. Kirk for their work on the issue in bringing the legislation before us. Their concerns are well placed.

We are looking forward to working through this bill. We are looking forward to hearing from the witnesses and, Mr. Chairman, I yield back the balance of my time.

MR. UPTON. Mr. Wynn.

MR. WYNN. Thank you, Mr. Chairman, for holding this very important hearing on Internet predators. I would also like to compliment the O and I committee for the work they have already done on this very important issue. You know, it is actually very refreshing to be discussing an issue with such a direct impact on American families, because in this committee we often hear from commercial interests basically promoting their bottom line. But I think we can do a great deal of good here today, and I hope we are able to work in a bipartisan fashion to produce a product that is helpful to all American families.

Let me just make an observation that of all the places our children go on the Internet, chat rooms are the most difficult sites for parents to monitor. These locations permit the kinds of persons you would usually avoid in person to easily and readily approach our children. One in four U.S. teen girls reported they had met strangers off the Internet. One in seven boys admitted that they did as well. While most of these Internet friends turn out to be another teen or preteen, that is not always the case. Unfortunately, children are now dying at the hands of the Internet child molesters and not all sexual exploitation occurs off line. At a disturbing rate, child predators are forming an online community, a bond that is unparalleled in history. They are openly uniting against legal authorities and discussing ways to influence public thinking and legislation on child exploitation.

In a 2000 study, the National Center for Missing and Exploited Children and the Justice Department said one out of every five children ages 10 to 17 surveyed said they received a sexual solicitation over the Internet during the previous year. I believe parents have primary responsibility. They must work to minimize the chances of this happening by monitoring the hours their children spend online. As a general rule, the later at night one is online, the more suspect the activity that occurs.

We should be sure to point out stories in the newspapers about cyber predators and make sure children do not give out information over the Internet that would lead a person to find out their child's true identity or their location, their address.

But government has an important role, and this is where this committee can do some real good. We must put together on a bipartisan basis a productive bill that will address this problem, not inhibit the use of the Internet, but make sure that predators cannot exploit the Internet for their nefarious purposes.

I look forward to hearing from the witnesses today and working on producing a quality bill. I relinquish the balance of my time.

[Prepared statement of Hon. Albert R. Wynn follows:]

PREPARED STATEMENT OF THE HON. ALBERT R. WYNN, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF MARYLAND

Mr. Chairman,

Thank you for holding this important hearing on Internet predators. Since we often hear from commercial interests promoting their ideas, it is refreshing to deal with an issue with a direct impact on families. Of all the places your child goes to on the Internet, chat rooms are the most difficult sites parents to monitor. These locations permit the kind of person you would usually avoid in person to easily and readily approach your children.

One in four US teen girls reported that they met strangers off the Internet. One in seven boys admitted they did as well. While most of these "Internet friends" turn out to be another teen or preteen, that's not always the case. Unfortunately, children are now dying at the hands of their Internet child molesters and, not all sexual exploitation of children occurs offline.

At a disturbing rate, child predators are forming an online community and bond that is unparalleled in history. They are openly uniting against legal authorities and discussing ways to influence public thinking and legislation on child exploitation. In a 2000 study, the National Center for Missing and Exploited Children and the Justice Department said that one of every five young people ages 10 to 17 surveyed said they had received a sexual solicitation over the Internet in the previous year.

Parents have primary responsibility to minimize the chances of this happening by monitoring the hours that kids can spend online. As a general rule, the later at night one is on line, the more suspect the activity that occurs. We should be sure to point out stories in the newspaper about cyber predators and make sure children do not give out information over the Internet that would lead a person to find your child in real life.

I look forward to hearing from the panelists today to find out more information on what can be done to stop this disturbing trend.

MR. UPTON. The gentleman from Pennsylvania, Mr. Fitzpatrick, is recognized for an opening statement.

MR. FITZPATRICK. Thank you, Chairman Upton and members of the committee, for permitting me to participate in today's hearing and for allowing me to address what I feel is a new and emerging danger to our Nation's children and their safety while using the Internet.

Your work in this area will help shed new light on this difficult problem that affects both law enforcement and America's families, and I appreciate the committee's dedication to this issue.

I first want to welcome David Zellis, Bucks County, PA's First District Attorney, to Washington and thank him for his participation today. David spent his life in a career prosecuting crime in my district, and I know that his testimony will be of great use and help to the committee today.

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

Recently, one aspect of the Internet has attracted a great deal of attention and considerable concern: the rise in popularity of social networking sites. Social networking sites, best known by the popular examples of MySpace, Facebook, and Friendster have literally exploded in popularity in just a few short years. MySpace alone has over 90 million users and ranks as the sixth most popular English language website, and the eighth most popular in the world.

While these sites were designed to allow their users to share virtual profiles of themselves to friends and like-minded users, social networking sites have also become a haven for online sexual predators who have made these corners of the Web their own virtual hunting ground.

The danger our children are exposed to by these sites is clear and compelling. According to a study conducted by the National Center For Missing and Exploited Children in 1998, there were 3,267 tips reporting child pornography. Since then the number has risen by over 3,000 percent to an astounding 106,119 tips in 2004.

The Department of Justice recognizes child pornography as a precursor for pedophiles and is often linked to online predators. According to Attorney General Gonzalez, one in five children have been approached sexually on the Internet. One in five children. On the face, these numbers are startling. Even more startling has been the visual evidence offered to millions of Americans through the news outlets like NBC Dateline's To Catch a Predator series.

Chris Hansen testified before this committee last month. However, the findings of his reports cannot be understated or forgotten. Throughout his investigations, Chris Hansen proved time and again, with disturbing regularity, that child predators are ready and willing to approach the prey they stalk online.

Who could forget the Dateline investigation in Florida where one predator arrived with his own 5-year-old son to meet what he thought was a 14-year-old boy?

Who can erase from their memory the man who entered the "Dateline" house naked, or the man who brought rope and duct tape with him for his encounter?

What would have happened in these circumstances if the children these predators were to meet were not decoys or if Chris Hansen were not there? How many assaults, rapes, and ruined lives would have resulted in these encounters?

Mr. Chairman, the fact, however disturbing it may be, is that child predators have harnessed the power and anonymity of the Internet and social networking sites to hunt for their prey. Something must be done to stop the spread of sexual predators online, and I believe that my legislation is a step in the right direction.

My legislation would limit access to minors to social networking sites in schools and in public libraries. However, this is no substitute for parental supervision, the first line of defense for our children's safety. That is why H.R. 5319 would require the FTC to design and publish a website specifically meant to serve as a clearinghouse for information for parents and educators. Finding a solution to the problem of sexual predators online and the Internet would take the combined efforts of parents, children, law enforcement, and the legislature to take action against these crimes; and it is my hope that the legislation that lead to the On-line Predators Act will assist in that effort. Thank you, Mr. Chairman.

MR. UPTON. The gentleman from Illinois, Mr. Kirk.

MR. KIRK. Thank you, Mr. Chairman, and thank you for having an appropriator on the committee here. I did do the customary courtesy--

MR. UPTON. Well, we supported the line-item veto here.

MR. KIRK. I did kiss the Chairman's ring before approaching the--

My involvement in this issue started from a unique source. I have a student leadership advisory board, made up of the junior and senior class presidents of my high schools. And I asked them, what is the biggest threat to kids that your parents do not know about? And they said it was MySpace.com.

Julie Wachtenheim, who is the student body president of Wheeling High School, said that she took a particularly good class picture and put it up on MySpace and within 45 minutes, a creep from Wheeling was trying to contact her. One of our students said that they felt that MySpace.com was really mycreepzone.com and it represented a unique danger to kids. That is outside the experience of nearly every Member of Congress who, when they grew up, did not have this threat to them.

I particularly want to admire the work of Congressman Fitzpatrick on this, a leader on suburban issues, and this legislation as well as several others are part of a bipartisan suburban agenda that we have. But this bill is particularly important because it was written by Congressman Fitzpatrick and cosponsored by Congresswoman Bean, representing a bipartisan view towards protecting kids in the 21st Century.

I would hope that the committee would remember we should have the conviction of our own convictions represented in 900 years of legal tradition, that we want a free and open discourse in a democracy, but our 900-year legal tradition also says that when you make money in doing business with children, you have a unique set of obligations to protect your customers and clients. And finding a way to apply that 900-year legal tradition of when you do business with children, the State has a unique role in making sure they are protected is what this legislation is about. So I applaud you, Mr. Chairman, for having it. Thank you again for having it.

MR. UPTON. I thank you again for your leadership and also Congressman Fitzpatrick and also Congresswoman Bean for their leadership on this issue.

We look forward to proceeding. At this point I would ask unanimous consent that all members of the subcommittee be allowed to submit their statements as part of the record and we are prepared now to listen to our panel of expert witnesses.

[Additional statements submitted for the record follows:]

PREPARED STATEMENT OF THE HON. BARBARA CUBIN, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF WYOMING

Thank you, Mr. Chairman. As a mother of two, this issue is of particular importance to me.

When my two sons were young boys in Wyoming, my husband and I worried about their safety all the time - like any parent does. We did our best to protect them when we could, but we could not be with them 24 hours a day. So we also did our best to teach them how to protect themselves from dangerous people and dangerous circumstances. But, boys will be boys, and we are still finding out about the risks my sons took. I thank God they are both alive and healthy today.

My family has come a long way since those days of worrying about being wary of strangers on the street, or looking both ways before crossing. Now parents and kids must be wary of strangers invading our computers and our technological way of life, making our very homes the target of their evil designs. I do not envy the work parents of young children must do to teach and protect their kids today. But just like my sons, kids will be kids, and the allure of the internet is too great to assume they will not experiment with it.

In many cases I am firm believer in state and local control over issues, but this is an interstate problem that requires an interstate solution. When predators can lure kids to ride a bus across state lines for the purpose of sexual exploitation, it is a problem that Congress must address. Similarly, I truly believe that parents are the single most influential people in kids lives. Just like efforts at stopping underage drinking, smoking and drug use, kids will respond to their parent’s teaching regarding internet safety. While

Congress can and should never replace parents as the role models for children, Congress can play a role in assisting parents as they struggle to raise children in the online age. That is the intention of this bill we are discussing today.

I am interested in hearing from the panelists if this particular legislation before us would result in any real reductions in online predatory activity. Would this legislation adequately help parents keep their children safe from predators? Are there other policies this subcommittee should be pursuing that would result in further protection of our children? Perhaps most importantly, are there solutions outside of legislation currently available in the marketplace that would protect children without undue restrictions on innovation and technology use? I look forward to hearing the opinions of the panelists.

Thank you again, Mr Chairman, for your leadership on this issue. I yield back.

MR. UPTON. We are going to be joined by the Honorable Greg Abbott, the Texas Attorney General; Ms. Parry Aftab, Executive Director of WiredSafety.org; Ms. Michelle Collins, Director of the Exploited Child Unit of the National Center for Missing and Exploited Children; Mr. Ted Davis, Director of Knowledge Asset Management, IT Department, from Fairfax County Public Schools; Mr. Chris Kelly, Vice President of Corporate Development and Chief Privacy Officer of Facebook; Ms. Amanda Lenhart, Senior Research Specialist for Pew Internet and American Life Project; Ms. Beth Yoke, Executive Director of ALA Young Adult Library Services Association from Chicago; and Mr. David Zellis, First Assistant District Attorney for the Office of Bucks County District in Pennsylvania.

We welcome you all. We appreciate you having submitted your testimony in advance. We would like you to take no more than 5 minutes to summarize your statement. I would note that the House is expecting votes within the next 20 or 30 minutes. So we will probably take a brief recess when that starts.

STATEMENTS OF HON. GREG ABBOTT, TEXAS ATTORNEY GENERAL; PARRY AFTAB, ESQ., EXECUTIVE DIRECTOR, WIREDSAFETY.ORG; MICHELLE COLLINS, DIRECTOR, EXPLOITED CHILD UNIT, NATIONAL CENTER FOR MISSING AND EXPLOITED CHILDREN; TED DAVIS, DIRECTOR, KNOWLEDGE ASSET MANAGEMENT, IT DEPARTMENT, FAIRFAX COUNTY PUBLIC SCHOOLS; CHRIS KELLY, VICE PRESIDENT, CORPORATE DEVELOPMENT AND CHIEF PRIVACY OFFICER OF FACEBOOK; AMANDA LENHART, SENIOR RESEARCH SPECIALIST, PEW INTERNET AND AMERICAN LIFE PROJECT; BETH YOKE, EXECUTIVE DIRECTOR, ALA YOUNG ADULT LIBRARY SERVICES ASSOCIATION; DAVID ZELLIS, FIRST ASSISTANT DISTRICT ATTORNEY, OFFICE OF BUCKS COUNTY

DISTRICT ATTORNEY, COMMONWEALTH OF PENNSYLVANIA

MR. UPTON. Mr. Abbott, we welcome you.

MR. ABBOTT. Mr. Chairman, and members of the subcommittee--

MR. UPTON. I think you just need to hit the mic button there too.

MR. ABBOTT. Thank you very much for the instruction. My name is Greg Abbott. I am the Attorney General of Texas, and I appreciate the opportunity to testify before you today.

I would like to very quickly follow up on a comment by Congressman Gonzalez from Texas. I think it is fair to say that from the brilliance and eloquence spoken by both you and Chairman Barton, I think it is clear that the draft drawers of new congressional maps in Texas, as we speak, should understand that there is no way you two should be paired against each other, so Texans can continue to benefit from the brilliance of both of you.

That being said, let me get right to the point, and that is that the dangers--

MR. UPTON. Mr. Burgess is on his way. He is a member of the committee as well, I want you to know.

MR. ABBOTT. You must be present to win.

The dangers to children created by social networking websites and chat rooms are all too real. Our experience in Texas is both illustrative and alarming. Three years ago we created a cyber crimes unit in the Texas Attorney General's office. Our goal was to find, arrest, and put behind bars child predators who use the Internet to stalk children.

A remarkable success is also tragic evidence of the risk children face when using chat rooms or social networking sites. Our investigators log onto chat rooms that are used by teenagers. Sometimes they log onto social networking sites, such as MySpace. The investigators typically assume the identity of a 13- or 14-year-old girl. Not long after they log on, and not long after they assume the identity of an underage child, they are barraged with uninvited, aggressive, and vulgar language.

The offensive Internet chat often turns into action. The predator sets a time, date, and location to sexually assault what he believes to be a 13- or 14-year-old girl. Now, on more than 80 occasions, the predator has shown up at the location of his choosing to act out on his criminal intent. The location is sometimes a motel, sometimes an apartment, sometimes a parking lot, sometimes other locations. And it is not uncommon for the predator to bring with him things like condoms, alcohol, or even a bed. Each of those more than 80 occasions has resulted in an arrest of a child predator by the Texas Attorney General's Office.

The 80th arrest was particularly notable. It was the arrest of a man who chatted with what he thought was a 13-year-old girl on MySpace. In reality, the graphic sexual conversations he was having were with a Texas Attorney General investigator. But what makes this case particularly frightening is that at the time he was arrested, the predator was out on bail from an arrest that had occurred 6 months prior. At the time of his most recent arrest, he was already under indictment for the solicitation of a minor. In other words, while he was out on bond, awaiting trial for illegal Internet solicitation of a minor, he was back on the Internet trolling for his next victim. This highlights how dangerous and incorrigible these predators are.

Children simply cannot be safe with the current landscape of cyberspace chat rooms and social networking sites. Unfortunately, not all the people chatting with predators are undercover officers and not all of the predators are caught in stings. Real children are real victims of real predators.

Recently a 14-year-old girl from central Texas was raped by a man she chatted with on a social networking site. Yesterday this story appeared on a TV station in Houston. To summarize it, the headline is "Woodlands Man"--Woodlands is a suburb of Houston--"Woodlands Man Admits He Seduced Teen Online." Quickly, the story says that Dale Beckham was charged with luring a 14-year-old boy he met over the Internet into a hotel room, where they had sex. Beckham traveled from his home in Houston to the Ottawa, Canada area with a laptop computer and digital camera. His home was later searched and authorities found hundreds of images of child pornography on his computers, including pictures of children younger than 12 engaged in sexual acts with adults.

Perhaps the most disturbing thing about these stories is that they are becoming all too common, so frequently posted in newspapers that the public may become desensitized to the reality, the harsh reality for the victim of Dale Beckham and the victims of thousands of predators across this country.

No one would allow their children to invite a predator over to the house for the evening. The fact is, that is exactly what happens when children log on to these social networking sites and chat rooms. Clearly, safeguards are needed at schools, at libraries, as well as in our homes if we are to protect our children against these predators. Such safeguards are the kinds of protections that Americans have come to expect. Streets, neighborhoods, and playgrounds are essential to our daily lives and are a part of the American social and economic fabric. Nevertheless, we must police our streets, neighborhoods, and playgrounds to ensure their safety.

Similarly, the Internet Super Highway and social network sites are vital to our modern-day economy and they provide an effective platform for exchange of ideas, information, and commerce. They also have developed into virtual neighborhoods where people can simply socialize. But these modern-day neighborhoods and playgrounds are proving just as susceptible to criminal predators as their traditional counterparts, if not more so.

Countless Federal laws aim to protect our streets and neighborhoods. The need to protect our virtual neighborhoods is just as great. It is time to end the games of pretend and denial. Even worse is that some use a nod and wink to imply it is the child's fault or the parents' fault when a child is victimized by someone they met online. Well, when a 14-year-old is raped in the streets, we don't blame the girl. Instead, we work to catch the rapist and work to ensure that we have safe neighborhoods where kids don't get raped. The scenario doesn't change just because the rape victim chatted with the rapist online.

Your ongoing vigilance is needed to protect children across this entire country and make the Internet a safe place for children to play, to learn, to explore, and to grow. We look forward to working with you to get that job done.

MR. UPTON. We look forward to working with you too. Thank you for your service.

MR. ABBOTT. Thank you.

[The prepared statement of Hon. Greg Abbott follows:]

PREPARED STATEMENT OF THE HON. GREG ABBOTT, ATTORNEY GENERAL, OFFICE OF THE ATTORNEY GENERAL, STATE OF TEXAS

Mr. Chairman and members of the subcommittee, my name is Greg Abbott, I am the Attorney General for the state of Texas, and I thank you for the opportunity to testify before you today.

Let me start by thanking you for shining a spotlight on the growing national nightmare of the Internet being used as a playground for child predators. Your legislative proposal – appropriately named "Deleting Online Predators Act" – is an important step towards making the Internet safer for our children and families. I wish the solution to the growing problem was as easy as hitting a delete button. Unfortunately, it is much more complex. With your active involvement, though, Internet safety will become more of a reality for millions of American children.

The dangers to children created by social networking websites and chat rooms are very real. The Texas experience is both illustrative – and alarming.

Three years ago, we created a Cyber Crimes Unit in the Office of the Attorney General of Texas. One of its primary missions was to find, arrest and convict child predators who use the Internet to stalk their prey. The unit's nationally recognized success is tragic evidence of the risk children face when using chat rooms or social networking websites.

Our Cyber Crimes Unit has investigators who log onto chat rooms that are used by teenagers. Sometimes they log on to social networking sites like MySpace. The investigators typically assume the identity of a teenage girl, usually around the age of 13 or 14. Not long after they log on and assume an under-age identity, they are barraged with aggressive and vulgar language that is uninvited. All too often, the offensive Internet "chat" turns into action. The predator sets a time, date and location to sexually assault what he believes to be a 13 or 14 year old girl. On more than 80 occasions, the predator has shown up at the location of his choosing to act out on his criminal intent. The location is sometimes a motel, sometimes an apartment, sometimes a parking lot, sometimes other places. It is not uncommon for the predator to bring things like condoms, alcohol, even a bed. Each of those 80+ occasions has resulted in an arrest of the child predator by the Texas Attorney General's office.

As an example, we recently arrested a 50-year-old man after he showed up at a Central Texas restaurant to meet what he thought was a 14-year-old girl. This predator had been talking with the girl – who in reality was one of our Cyber Crimes investigators – in an online chat room. He even stopped on his way to the meeting and bought some wine coolers to give the girl.

And not long ago, we arrested a 52-year-old university professor at a bus station in McAllen, Texas, where he was waiting for what he thought was a 13-year-old girl he met online. He even bought the would-be teenager a bus ticket so she could travel from miles away to meet him.

The 80th arrest was particularly notable. It was the arrest of 27-year-old John David Payne, who had been chatting with what he thought was a 13-year-old girl he met on MySpace. In reality, the graphic sexual conversations he was having were with a Texas Attorney General investigator.

What makes his case particularly frightening – although sadly not unusual – is that, at the time of his arrest, Mr. Payne was out on bail from an arrest that occurred six months prior. In fact, at the time of his most recent arrest, he was already under indictment for online solicitation of a minor. In other words, while he was out on bond awaiting trial for illegal Internet solicitation of a minor, he was back on the Internet, trolling for his next victim. These child predators are dangerous and incorrigible, and children simply cannot be safe with the current landscape of cyberspace chat rooms and social networking sites.

Unfortunately, not all of the people chatting with predators are undercover officers, and not all of the predators are caught in stings. Real children are real victims of real predators. Recently, a 14-year-old girl from Central Texas was raped by a man she chatted with on a social networking site. This is just one of the most recent examples, examples that are repeated around the country with increasing frequency.

As we hold this hearing today, millions of teenagers are chatting online, posting personal information on a profile page, talking to other teens on social networking sites, and meeting people in chat rooms. Before we leave here today, countless of those teens will have innocently chatted with someone they didn't know. And, before we leave today, some of those unknown chatters will turn out to be predators who have just located their next target.

Clearly, safeguards are needed at schools and libraries – as well as in our homes – if we are to protect our children against these predators. Such safeguards are the kinds of protections that Americans have come to expect.

Streets, neighborhoods and playgrounds are essential to our daily lives and are part of the American social and economic fabric. Nevertheless, we must police our streets, neighborhoods and playgrounds to ensure their safety. Similarly, the Internet superhighway and social network sites are vital to our modern day economy and they provide an effective platform for the exchange of ideas, information and commerce. They also have developed into virtual neighborhoods where people can simply socialize. But, these modern-day neighborhoods and playgrounds are proving just as susceptible to criminals and predators as their traditional counterparts, if not more so.

As can be expected, the responsibility for protecting children and teens who use the Internet is a shared responsibility. Law enforcement will continue to improve its efforts to track down, arrest and put behind bars anyone who uses the Internet to harm children.

Parents are also a part of the process. Parents must use oversight, education and vigilance to protect their children. Just as parents warn children not to take candy from strangers and to look both ways before crossing the street, parents must warn children about the dangers that exist on the Internet. Parents frequently evaluate whether their teen is sufficiently responsible with a car before allowing him or her to go driving. One reason, of course, is that teens, if driving irresponsibly, could hurt themselves or others. The same is true with the Internet. Parents should ensure that their teenagers are sufficiently informed and responsible in their Internet use. Otherwise, they could get hurt.

But the great weight of the problem must be shouldered by the very creators and hosts of these networking sites and chat rooms that provide the previously non-existent opportunity for child predators. Social networking sites and chat rooms have created an environment in which predators target their next victim and plot their next attack. Predators use these web locations as a starting point for raping a child! The creators and hosts of these networking sites are not the predators who commit the crime, but they create the opportunity for the criminal to carry out his crime.

The creators and hosts of these networking sites are part of the problem, and as part of the solution they must do more than pay lip service to providing a safe environment for children. They must take affirmative, definitive action to ensure the protection of children who use their sites and chat rooms. They can no longer be allowed to turn a blind eye to the predators who lurk on the playground they created.

Admittedly, some of these networking sites and chat rooms have *begun* the process of a constructive dialogue to address the issue. But, if they are honest, they will admit that the predator problem persists, and that there is more they can do to solve the problem.

As mentioned earlier, parents have a role to play. But parents are being denied some of their ability to play that role. The networking sites should structure their systems so parents can block access to their sites. Parents across the country prevent their children from going to locations where crime may occur, where sex and drugs may be traded, or where their children could be harmed. Parents should not be denied that opportunity (that responsibility) simply because the location is in a virtual neighborhood, rather than a neighborhood down the street. If parents want their children to have the opportunity to participate on the networking sites, the sites should be offer parents filtering software to block their child's access to content and websites that parents deem inappropriate.

Heightened precaution must be taken to protect children under 16 from child predators. Should networking sites really mix 13 year old children with adults who are participating in the networking site for the purpose of looking for a sex partner? To avoid this problem, the sites should be structured so that only children over a certain age can participate in sites with adults.

Children who use the sites should not be subjected to sexually explicit images and solicitations, or other age-inappropriate material. The sites should be structured so that such material is not accessible without age verification.

While social networking sites are a lot of fun for kids – and have the potential to expose our children to a world of knowledge and bring them literally worldwide friends – many of the sites also subject children to a world of predators, pedophiles and pornographers.

As law enforcement officers, we are asking that social networking sites and chat rooms more effectively police themselves, or be shut down. Our society does not tolerate houses of prostitution. Neither should it tolerate virtual houses that promote predators.

Computer literacy and Internet access are necessities, not luxuries. And without question they have made our lives better. But the anonymity of the Internet has created opportunities for child predators and child pornographers, giving them cover to act on their perversions.

It turns out that the Internet, for all of its benefits and all of its conveniences, is still a pretty dangerous place. It would not be an exaggeration to say that no child is safe from the unwanted advances of chat room predators, men who use the Internet in an attempt to realize their worst fantasies.

Thank you for working to protect children from the nightmare of these predators. We look forward to working with you to win the war against those who threaten the safety of our children, our families, our homes and our communities.

MR. UPTON. Ms. Aftab.

MS. AFTAB. Good morning, Mr. Chairman. Thank you so much. WiredSafety is honored to be represented on the panel today. We spoke at the first day of the Oversight and Investigations Subcommittee, and yesterday I was honored to speak again at the field hearing, which was a much closer commute to my house in New Jersey.

I am an Internet privacy and security lawyer, at least by training. I was one of the first Internet lawyers in the world, and I used to earn a good living. I represented many of the big corporations that you hear from, and I used to protect them in cyberspace.

In 1998, somebody sent me a link to a website. It was a child pornography website, and I clicked on the link and I saw a picture of a 3-1/2-year-old being raped. I cried for a while. I vomited a little bit longer, and I said I might be able to do something if the corporations that were paying me so well to protect them online might listen to me instead of charging a lot of money. I would give away my time to see if we could protect children and, at the same time, made sure they had access to this wonderful technology; because online all children can walk, talk and see, all of them have access to the world. And that was a challenge. But as a lawyer who was very well paid in this area, I was always good at challenging the risks and benefits of the technology.

Luckily, 11,000 people joined me. We are all unpaid volunteers. We operate in 76 countries around the world. We don't have real offices. We have no paid staff. We are just people who care a great deal about protecting each other, especially our children.

Now, we have also been inside the social networks. Since I first called MySpace in February of 2005, screaming about things that I saw they were doing when they had 6 million users. And they called me back saying, "Kids? We don't want kids. It is designed for independent musicians. We can't handle them. They are doing all these things. What to do?" I said you have to do some things. You have to have a law enforcement policy and guide. I wrote it for them. It is used as the model for their work with law enforcement around the country. I said, you need safety tips. I wrote them in the middle of the night. They had typos with them for 6 months. We put them on their site until they knew enough to take over and put their own there. And my volunteers answered questions from parents when they became concerned about social networks. When they came from 6 million to 90 million, we became involved in all of the other social networks.

The second one was Facebook. When Chris Kelly came into Facebook, Chris and I knew each other for several years and we said we will help you, too, because I know how serious they take this. We are now embedded with all the major social networks of the world as the watchdog, trying to get them to beef up best practices. The bill specifically is so well intentioned.

And I met Congressman Fitzpatrick yesterday. I know where it is coming from. The problem is, you need to understand both kids and social networks. There is no ISP in this country or major entertainment site or major brand that isn't either already using a social network technology or contemplating it. I receive several phone calls a day from both venture capitalists and investors, telling me that the sites that are coming to them for money will not be funded unless we get in on the inside and tell them what they need to do. So they are out there.

If this law were implemented as written, they would be blocking Microsoft, Yahoo!, Google, AOL, all of the major networks, Viacom, every single one that you can imagine, not just the new ones that are social networking only.

In addition, as we look at the technology, kids are doing it for a number of reasons. For years I have spent time protecting children from adult predators. That is why I got into this. And then I started protecting children from each other, cyber bullying. Congressman Shimkus was kind enough to put together a special event with Al Roker and my Teen Angels and us on cyber bullying. Cyber bullying has exploded. It is the biggest problem you find on social networks, not the sexual predators which gets a great deal of hype, but kids are being victimized right and left on social networks as they are cruel to each other. And now we are finding the kids are hurting themselves, posting things that might have sounded cool at slumber parties, or they were drinking too many bottles of beer, and it might affect them getting into Stanford or something else because they posed as drunken sluts, because it sounded like a good idea at the time. It is not cool to say you were home baking cookies with your 5-year-old niece. It is a lot more fun to say you were doing something more outrageous, and you can do that on your MySpace.

As we looked at this, we are all unpaid volunteers. We are largely unfunded. We realize we have to come up with solutions that will work quickly. And although the law is well intentioned, I think that perhaps as we tweak it, if you are looking for something that will compel schools and libraries, what we should do is to get schools to adopt a risk management plan. Say to them these are the real risks, this is how it works, here are the models. Send home an acceptable use policy to the parents, saying if your kids are cyber bullying each other from a home computer, but it impacts school, we have the right to do something about it. Let's get them to do something meaningful, and the schools rather than legislators can decide what is right for that particular school.

In addition, we have gone to the true expert on the Web. Marvel Comics has donated Spider-Man as our spokesman, and we have a new comic coming out on social networking that we think will be effective. We have gone to kids, Teen Angels is our program. Kids talking to each other can be very effective. The kids said that they never thought smart kids could be caught. So we have been doing a great deal of work on that and we have a series of animations, one of which I would have shown you if I could get my computer to work. So much for being a techno lawyer. It says that cute 14-year-old boy may not be cute, may not be 14, and may not be a boy. We have an animation where a girl is talking to heartthrob Bob on her social network page. In one section, it is a fat slob sexual predator and another one it is three mean girls cyber bullying, setting her up for humiliation. In the third, it is her 8-year-old bratty brother and his friend who want to show up with a video camera when she goes to the meet. We have someone who is out on a day pass from prison. Unfortunately, Christina Long, the first girl who was killed by an Internet sexual predator, confirmed 4 years ago, after the person was in prison awaiting sentencing, he was trying to lure other 13-year-olds from prison.

What do we do? We look for folks, people like Nick Lachey. He is our new spokesperson. The kids like that a lot. We have the new Ms. Virginia, Adrian Scarlotta. We have looked to our new program that came out of the hearings, the Oversight and Investigations hearings. It is called WiredMoms. It is our Moms Against Internet Sexual Predators. We have found that by mobilizing people, giving them the tools they need, including our new Internet safety plan that will launch in September, parents can put in the information they have, the age and genders of their kids, what they are doing, what their values are, and it will spit out a road map of what they need on a technology site so they can know how to talk to their kids and know what to do

If we can make it easy, we can make it clean, we can make it accessible, we can all get involved. We can make a difference. And for the first time--I have been doing this for 10 years--and for the first time, Congress is leading the world. I do this all over the world. They do it in Singapore, England, Hong Kong. I work with parents to promote a guide for Internet safety. Now, finally, all of the talents of these great groups, national centers, all of these fabulous people who I have been admiring for the years have been bringing before Congress. It is time.

Let us work together. I am WiredSafety and our Teen Angels and Wired Moms and Spider-Man, and you name it, we are working together on this. You come up with any issues you want, I will sit down and help you plot, kick the tires, and let you know what is going on.

Our new program for the social networks, letting you know who is doing a good job and who isn't, will launch in September to let you know what is going to make it a little easier.

[The prepared statement of Parry Aftab follows:]

PREPARED STATEMENT OF PARRY AFTAB, EXECUTIVE DIRECTOR, WIREDSAFETY.ORG

SUMMARY

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

With our children walking around with Internet access in their backpacks and pocketbooks, we can no longer rely on parents watching whatever they do from a central location computer. Our children need to learn to use the "filter between their ears" and "ThinkB4TheyClick." This requires that we get them involved in framing solutions and educating each other. It also requires that we find new ways of building good cyber-citizenship and helping the kids and parents spot risks in new technologies and protect themselves online. It also requires that we engage the Internet industry itself in ways to build safer technologies and adopt best practices designed to make all their users, not just children, safer.

Social networking, a combination of mini-web pages, blogs and searchable communities, have expanded in recent years, most recently exploding with the growth of MySpace.com. Parry Aftab estimates that more than half of the young teens in the US with home Internet access have at least one social networking profile. Some were set up by their friends, and others by the young teens themselves. Many have 2 to 5 separate profiles on just one site, and most have at least one profile on two or more social networks (not all being used, however). WiredSafety.org first began its social networking safety work in 2004, after learning how many young teens and preteens were beginning to use them. Unlike the early AOL profile pages used by teens and preteens in prior years, where the young users could post their contact information and brief statements about their interests, these networks were designed to be interactive. And instead of dry posts of contact and other personal interest information, these networks allowed teens to use html coding to add music, movies, animations, sounds, images and lots of user generated content to their page.

While the media and many others have focused only on the dangers of these networks when used by preteens and teens, it is important that we also explore their good uses and value and why their use has exploded in the last year and a-half. We have spent two years studying how and why preteens and teens use these kinds of sites.

Most use them for innocent purposes. They want to find their friends and communicate among larger groups than they can do via instant messaging. They can post something and know everyone in their class or group can read it at the same time. They want to show off their creativity and how special they are. And they can pretend to be prettier, more popular, richer and more famous than they are in real life. They raise money for their favorite charity and awareness for new causes.

They can post one message and their 150 best friends can see it right away. Unfortunately, so can those who might not have their best interests at heart. And sadly, in some cases, our teens are acting out, taking risks and seeking romance online (even knowingly with adults). That's when things can get dangerous, especially for young teens.

Our preteens and teens are often intentionally sharing risky information online in profiles, blogs and on websites. They may also share this information with stranger unwittingly, such as posting their cell numbers on their public away messages when using IM technologies. They intentionally post graphically sexual images and engage in and post cybersexual communications on their profiles and in chat-type technologies. And even when they are careful about protecting their own privacy, they may not be safe from their friends - even well-meaning friends. Their close friends may expose personal information about them by posting photos and information on their profiles.

They are also, in greater and greater numbers, meeting people offline that they met online. In 2000, Family PC Magazine reported that 24% of the teen girls they polled and 16% of the teen boys they polled admitted to meeting Internet strangers in real life. I believe that these numbers, when revised, will disclose that many more are doing this than 5 years ago. It is becoming more commonplace. Our children go willingly to offline meetings with these people. They may think they are meeting a cute fourteen year old boy, but find that they are meeting a 47- year old child molester instead. This has to stop.

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

And while we focus on sexual predators online and how they are using social networks and community interactive technologies to reach our children, we too often forget that the most prevalent risk our children face on these networks and using these technologies is cyberbullying, not adult sexual predators. A vast majority of the preteen and young teens we polled have been involved, directly or indirectly, in at least one cyberbullying incident. They torment and terrorize each other. They threaten and embarrass each other. They post fake profiles, hateful messages and steal each other's passwords and identities, all designed to bully their victims. They do it in groups, singly, openly and anonymously. They use cell phones, interactive gaming devices and sites and web profiles, blogs and websites where you can vote for the ugliest, fattest, least popular or gayest student. And schools are the ones most impacted, when students who might be creating and posting these hateful communications from home or otherwise outside of school ground and after-hours, become engaged in violence and hurtful interactivities during school hours. In addition, when our teens and preteens are posting real or fantasy information about how much alcohol they consumed at this weekend's party, or how active their sex life has become, or how they cheated on their finals or shoplifted from the local mall, they may not realize that college recruiters, scholarship committees, coaches and future employers can access this information in years to come. This is an increasingly growing risk our children pose to themselves.

All of this has schools concerned. Private schools, especially, are facing real challenge controlling their students' activities online. Facebook.com is favored by private and parochial school students, who are impressed with the fact that it was formed at Harvard and other private and parochial students can be found there. It has, as some teens tell us, the “snob factor.”

Our children are sometimes accessing these sites from their school laptops, in-classroom desktops and school and public libraries. So, a parent's “house rules” may not have much effect when their child leaves the house. So, creating a new law prohibiting schools and libraries from allowing underage students and users to access these sites is an obvious approach. But is the answer to these problems found in laws restricting where students can go during school hours on school computers? Or can this be controlled by blocking access to interactive community networking sites, such as MySpace, Facebook and others from public and school libraries? While this may appear on its face to be an easy answer, it is neither easy nor the answer.

As more social networks are launched every day, and every ISP, entertainment company and wireless provider is either building a social network or finding a way to integrate social networking and community interactivity into their new and existing sites, it is impossible to block all of them and not other valuable Internet features, sites and content. Instead, schools need to be armed with the tools and risk management expertise to decide what sites their students can access during school hours from their servers and how to enforce their decisions and policies.

Schools need to decide if their students should have access to *any* non-educational site from school computers, and if so, which ones and for what purpose. They then need to develop a policy communicating this decision and the rules to the students (in language they understand), the teachers, the parents and other caregivers and to their IT team. They need to decide whether they will be using software to help enforce their policy, or merely traditional discipline for violating school policies. That too needs to be communicated to the school community. They also need to create or adopt educational programs teaching their students what information they can and shouldn't be sharing online, the risks of irresponsible Internet use and where to go when things go wrong. They can play an important role in teaching parents and other community members about safe, private and responsible Internet and wireless technologies use.

Educators, not legislators, should be deciding what students do during the school day. They know their students and the learning environment best. But schools do need the guidance and help of legislators and regulators to do this right. They need reliable information and studies on which they can base their decisions. They need to be apprised of new trends and developing risks. They need to know that websites and services are using the latest and best technologies and have adopted the best industry practices with their users' safety in mind. They need help that Congress can provide.

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

Creating a central reporting database where all instances of cybercrimes are reported for statistical purposes, from cyberharassment to Internet-related ID theft, fraud and scams, to sexual predators and Internet-related child pornography and sexual exploitation would be incredibly helpful. It could track cybercrime trends affecting adults, seniors and youth. It could be used to help design safer systems and best practices and guide legislation directed at a meaningful problem, in a meaningful way.

In addition, with tax dollars becoming more and more precious and the mission of all Congressional representatives to put tax dollars into the most effective use, existing programs by trusted non-profit groups can be highlighted and made available online to schools and community organizations that need them, without cost. Without having to reinvent the wheel, massive amounts of programs, lesson plans and risks management guides already exist that can be used as is, or easily retooled. Finding a way to get these wonderful resources into the hands of those who need them the most, using interactive technologies and the Internet and mobilizing volunteers to help deploy existing programs that were developed with or without government dollars is the fastest way to make a dent in the problem. Focusing attention on what works and what doesn't is something that Congress does best. WiredSafety.org and I pledge our help in doing that.

It's time.

OPENING STATEMENT

SOCIAL NETWORKS AND COMMUNITY INTERACTIVE TECHNOLOGIES AND US TEENS AND PRETEENS

WiredSafety has been involved in cybersafety for ten years (see the attached description of our organization and work in the Appendix). It was founded and is run by Parry Aftab, one of the first Internet lawyers specializing in security and privacy law. She is frequently referred to as “The Kids Internet Lawyer” for her work with the children's online industry and child privacy issues and is an unpaid volunteer. For ten years we have cautioned Internet users of all ages against sharing too much personal information online, through profiles (pre-social networking), websites and online and mobile chat technologies. So we could quickly adapt our expertise to the new social networking explosion. It is crucial that this Sub-Committee recognizes that social networking is the future of the Internet and cyber-communications. It is here to stay and being used by every major ISP and cyber-industry, by every trusted brand online and offline. It is not limited to newcomers, such as MySpace and Facebook, but includes Google, AOL, Microsoft, Yahoo! and others. Coming to terms with how and why people are using these networks is essential.

There are always trends in what kids are doing online. And some, that may have started as a trend, become core technologies adopted by adults and businesses alike. Instant-messaging and social networks head this list. Social networks (sometimes incorrectly called “blogs”) are the future of the Internet and cyber-technology. They are a cross between an online diary, a cyberdating network, an online publishing house, the fastest way to reach out to your friends online and a place to share your creativity and express yourself – on steroids.

MySpace grew in popularity because it offered what teens wanted - the ability to express themselves in any way they could imagine if they could locate or write the code to do it. But, interestingly enough, when MySpace was created, it was designed for independent musicians age 18 - 34, not for teens and preteens. It was the teens who found MySpace, not the other way around. By February 2005, when I first called them with our concerns, MySpace had approximately 6 million users/profiles. By late May, 2005, they had approximately 23 million users/profiles. By the end of 2005 that had increased to approximately 50 million users/profiles and stands at about 90 million users/profiles today. Until recently, our safety tips appeared on MySpace as their safety page, and we were the only watchdog within the site. We remain the only watchdog within most of the other major social networks, but no longer populate MySpace's safety pages or take abuse reports from their users. This is now handled internally by MySpace.

MySpace.com and other similar sites are designed to allow people to share their creativity, pictures, and information with others. It also allows them to network with others online. Sometimes people do this to find romance. Sometimes they do it to find friends with similar interests. While this may be okay for adults, it is not okay for kids and may not be okay for young teens without parental supervision.

Most social-networking websites agree and prohibit anyone under a certain age from using their website. Unfortunately, while they may set rules to keep younger teens and preteens off the site, they can't prevent kids from lying about their age and pretending to be old enough to use the website. (These sites are typically free and, without a payment or age verification or authentication, they never know who their members are in real life.) To address the lying some sites have developed special software applications designed to help identify underage members by reviewing the contents of member profiles. It's not perfect, but it does help spot many underage members.

I recently visited a Marine Base in Yuma, Arizona and worked with teens and preteens on the base. I polled many of the preteens, learning that several of them had a "MySpace." When I pointed out MySpace's minimum age requirement of 14, they shrugged and explained that they were "mature for their age." After a 45-minute presentation, these same preteens knew far more about protecting themselves on MySpace and similar sites. But they still wanted to keep their "MySpace" profiles. This is a problem parents, schools, library media specialists and others are facing. How do you keep preteens and teens off of the social networks? Parents are told to talk with their kids,

While no one can always tell if someone is lying about their age, some of these sites use some method of age verification or authentication (such as Facebook.com's college e-mail address requirement for their college users or YFly.com's field team approach). And these and others really try to keep underage users off their site. Many other similar sites do not. So, when allowing any teen to use a social-networking website, even with supervision, it helps to make sure it's a trustworthy one. WiredSafety allows those we consider more trustworthy to use our safety tips and link to our help teams. So, looking for our tips is a good way to start finding the sites we consider more trustworthy. In addition, our new seal program that will review sites for compliance with best practices, privacy and safety practices will launch in September.[1] This should help in telling the good and responsible players from the bad and irresponsible ones.

All ISPs, entertainment companies and major wireless providers either already have a social network or similar community feature or will over the next year. New ones are launched daily. I am contacted by leading venture capitalists and investor groups daily to advise on a new proposal or network. The top five or six networks with substantial US user-bases claim, collectively, almost 200 million user profiles. Even if one user may set up several profiles (I have learned that most 12-16 year olds have between 2 and 5

[1] The seal will deal with several issues impacting safety, such as their law enforcement policies (how easy it is for law enforcement agencies to work with the site when cybercrimes and abuses are reported or in conducting investigations, how long they maintain IP data to assist in tracking the identity of cybercriminals and the location of missing children, and how well they inform law enforcement about what information they collect and retain and how to legally request it), safety (privacy and security settings, abuse reporting mechanisms, the expertise of their abuse reporting staff, their terms of service and how well they are enforced), their customer service (how they handle request from parents and schools, how easy it is to remove or modify a profile, how well they educate their users about safety and security, their technological protections against malicious code and ID theft, and their relationship with high-risk sites) and if they cater to preteens or teens, how carefully they care for their interests (such as how well they comply with the child-protection privacy rules and laws and how sensitive they are to appropriate marketing and advertising practices and placement and how well they handle cyberbullying and other youth-centric abuses).

different profiles, each set up with a different e-mail address), it is estimated that at least 80 million people are using social networks in the US.[2] I have polled approximately 10,000 teens and preteens face-to-face across the US over the last four months on their social network usage. These sites include MySpace.com, Xanga.com, Bebo.com, Tagged.com, BlackPlanet.com and its sister site, MiGente.com, and FaceBook.com, among others.

We have learned a great deal about why kids use these kinds of sites. Most use them for innocent purposes. They want to find their friends and communicate among larger groups than they can do via instant messaging. They can post something and know everyone in their class or group can read it at the same time. They want to show off their creativity and how special they are. And they can pretend to be prettier, more popular, richer and more famous than they are in real life. They raise money for their favorite charity and awareness for new causes. They stage protests from their profiles new millennium-style, letting policymakers know how they feel about the propose immigration policies and other issues important to teens, in interactive petitions. They make and share news. They engage in educational activities, such as building profiles of their favorite historical characters. One user may write music and another he has never met may write the lyrics. It's where they hang out and have fun, share their expertise and talents and find others like themselves. Or, they may be looking for other teens with lives radically different from theirs - farm-kids may want to find city-kids or conservative kids may want to find outrageous ones. They can try on different guises and lifestyles and pretend to be someone they aren't, both good and bad.

They can post one message and their 150 best friends can see it right away. Unfortunately, so can those who might not have their best interests at heart. But most of our teens aren’t there for meeting strangers or checking out provocative photos. Sadly, in some cases, though, they are acting out, taking risks and seeking romance online. That’s when things can get dangerous, for users of all ages, but especially young teens. (You can learn more about Internet sexual predators and how they operate at our new site for preventing and helping young victims of Internet sexual predators, Katiesplace.org.)

Most use them for innocent purposes. They want to find their friends and communicate among larger groups than they can do via instant messaging. They can post something and know everyone in their class or group can read it at the same time. They want to show off their creativity and how special they are. And they can pretend to be prettier, more popular, richer and more famous than they are in real life. They raise money for their favorite charity and awareness for new causes. They stage protests from their profiles new millennium-style, letting policymakers know how they feel about the propose immigration policies and other issues important to teens, in interactive petitions. They make and share news. They engage in educational activities, such as building profiles of their favorite historical characters. One user may write music and another he has never met may write the lyrics. It's where they hang out and have fun, share their expertise and talents and find others like themselves. Or, they may be looking for other teens with lives radically different from theirs - farm-kids may want to find city-kids or

[2] Some websites, including MySpace.com, make it very difficult to remove a profile. In MySpace's case, the user must fill out an online form to request instructions on profile deletion and a special code will be e-mailed to the non-MySpace e-mail they used when setting up their account for them to use to shut down their profile page. Due to the fact that many users either use a fake e-mail address to protect their privacy or have since stopped using the one they provided when the account was set-up, the code cannot be delivered. Even if the e-mail address is real and still functioning, however, many ISPs and e-mail providers block MySpace communications sent over their networks as SPAM. Without the code, the profiles remain up, even if the user wants them removed, which may lead to inflated user-numbers. (WiredSafety has arranged for a special process to assist in the removal of teen/preteen profiles when the e-mail address is not working, but I suspect that it is not widely used unless the user comes to us for our assistance.)

conservative kids may want to find outrageous ones. They can try on different guises and lifestyles and pretend to be someone they aren't, both good and bad.

They can post one message and their 150 best friends can see it right away. Unfortunately, so can those who might not have their best interests at heart. And sadly, in some cases, our teens are acting out, taking risks and seeking romance online (even knowingly with adults). That’s when things can get dangerous, especially for young teens.

Our preteens and teens are often intentionally sharing risky information online in profiles, blogs and on websites. They may also share this information with stranger unwittingly, such as posting their cell numbers on their public away messages when using IM technologies. They intentionally post graphically sexual images and engage in and post cybersexual communications on their profiles and in chat-type technologies. And even when they are careful about protecting their own privacy, they may not be safe from their friends - even well-meaning friends. Their close friends may expose personal information about them by posting photos and information on their profiles.

They are also, in greater and greater numbers, meeting people offline that they met online. In 2000, Family PC Magazine reported that 24% of the teen girls they polled and 16% of the teen boys they polled admitted to meeting Internet strangers in real life. I believe that these numbers, when revised, will disclose that many more are doing this than 5 years ago. It is becoming more commonplace. Our children go willingly to offline meetings with these people. They may think they are meeting a cute fourteen year old boy, but find that they are meeting a 47- year old child molester instead. This has to stop.

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

And while we focus on sexual predators online and how they are using social networks and community interactive technologies to reach our children, we too often forget that the most prevalent risk our children face on these networks and using these technologies is cyberbullying, not adult sexual predators. A vast majority of the preteen and young teens we polled have been involved, directly or indirectly, in at least one cyberbullying incident. They torment and terrorize each other. They threaten and embarrass each other. They post fake profiles, hateful messages and steal each other's passwords and identities, all designed to bully their victims. They do it in groups, singly, openly and anonymously. They use cell phones, interactive gaming devices and sites and web profiles, blogs and websites where you can vote for the ugliest, fattest, least popular or gayest student. And schools are the ones most impacted, when students who might be creating and posting these hateful communications from home or otherwise outside of school ground and after-hours, become engaged in violence and hurtful interactivities during school hours. In addition, when our teens and preteens are posting real or fantasy information about how much alcohol they consumed at this weekend's party, or how active their sex life has become, or how they cheated on their finals or shoplifted from the local mall, they may not realize that college recruiters, scholarship committees, coaches and future employers can access this information in years to come. This is an increasingly growing risk our children pose to themselves.

Our preteens and teens are often intentionally sharing risky information online in profiles, blogs and on websites. They may also share this information with stranger unwittingly, such as posting their cell numbers on their public away messages when using IM technologies. They intentionally post graphically sexual images and engage in and post cybersexual communications on their profiles and in chat-type technologies. And even when they are careful about protecting their own privacy, they may not be safe from

their friends - even well-meaning friends. Their close friends may expose personal information about them by posting photos and information on their profiles.

They are also, in greater and greater numbers, meeting people offline that they met online. In 2000, Family PC Magazine reported that 24% of the teen girls they polled and 16% of the teen boys they polled admitted to meeting Internet strangers in real life. I believe that these numbers, when revised, will disclose that many more are doing this than 5 years ago. It is becoming more commonplace. Our children go willingly to offline meetings with these people. They may think they are meeting a cute fourteen year old boy, but find that they are meeting a 47- year old child molester instead. This has to stop.

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

And while we focus on sexual predators online and how they are using social networks and community interactive technologies to reach our children, we too often forget that the most prevalent risk our children face on these networks and using these technologies is cyberbullying, not adult sexual predators. A vast majority of the preteen and young teens we polled have been involved, directly or indirectly, in at least one cyberbullying incident. They torment and terrorize each other. They threaten and embarrass each other. They post fake profiles, hateful messages and steal each other's passwords and identities, all designed to bully their victims. They do it in groups, singly, openly and anonymously. They use cell phones, interactive gaming devices and sites and web profiles, blogs and websites where you can vote for the ugliest, fattest, least popular or gayest student. And schools are the ones most impacted, when students who might be creating and posting these hateful communications from home or otherwise outside of school ground and after-hours, become engaged in violence and hurtful interactivities during school hours. In addition, when our teens and preteens are posting real or fantasy information about how much alcohol they consumed at this weekend's party, or how active their sex life has become, or how they cheated on their finals or shoplifted from the local mall, they may not realize that college recruiters, scholarship committees, coaches and future employers can access this information in years to come. This is an increasingly growing risk our children pose to themselves.

All of this has schools concerned. Private schools, especially, are facing real challenge controlling their students' activities online. Facebook.com is favored by private and parochial school students, who are impressed with the fact that it was formed at Harvard and other private and parochial students can be found there. It has, as some teens tell us, the “snob factor.” Teens need to be on a social network to have a social life these days. (Although many are leaving MySpace in favor of other sites, for various reasons.)

But there’s more to it. When I polled an average of 5000 kids every month on this, I learned that they love the creativity of it. They love expressing themselves so others can appreciate it. They enjoy adding sparkly graphics and sharing their stories, poems and jokes. One of the Teenangels (WiredSafety’s expert teen and preteen program, teenangels.org) told me that it’s all about “Pink! Pink! Pink!” She can build a page using pink font, on a black background and feel creative and cool. (Her mother is an interior decorator and she has to wear a school uniform, and saw this as her sole expressive outlet.)

As important as allowing them to express themselves in a creative way is, though, it’s not enough to get me to do a turn-about with these kinds of sites and teens. I was very negative about these sites. I have now taken a second look after talking to another one of my Teenangels.

This Teenangel (a soft-spoken and gentle girl) did a research project on social networking websites. She reviewed some of these sites and listed the kinds of risks young teens face on these websites. She then went on to explain that she had several profiles online at these sites. I was initially shocked and disappointed that one of my expert teens would take such risks with their personal information when they knew better. When I asked her why she would do such a risky thing, as the Teenangels often do, this one taught me something new.

She explained that it's hard being a young teen these days. Few kids in the school will give you the chance to see how much you have to offer unless you are the captain of the cheerleading squad or of the debate team. A profile page that is open to the other students at your school gives you a chance to share the special things about yourself with them, and will help them get to know you better. It's about sharing your favorite movies and books, about sharing fun vacation memories and your dreams, it's about sharing how special you are. It's about helping you make friends in your school with people who appreciate you. It's not about strangers, it's about others in their class.

There is a real value to that. Whether it's by posting a profile page that is supervised by their parents, or building a website. It can be pink and sparkly, or thoughtful and inspiring. But it's all about who your teen is or who they want to be. It's a challenge to give them a place where they can express themselves while keeping them safe, protected from predators and from sharing too much private information online. But if you are willing to supervise what they are saying and doing on their profiles, I'm willing to help.

Lying on their pages is part of what this is all about, too. They pretend to be older (and not just to get around the age restrictions), richer, more famous or more popular. Boys pretend to be girls and girls pretend to be boys. They may be tall blonde surfers from Malibu or live on a ranch in New Zealand. While this may not be a problem, some of their other kinds of pretending can be dangerous for teens in a public social network.

They may act tougher than they are in real life "rl," provoke other, or talk about getting drunk, or their sexuality. They may pose as someone they don't like, to cyberbully and harass them, or steal their identities. I have spent years protecting children from predatorial adults. I never thought I would be spending as much time as I am protecting them from each other. But, they are using these sites by the millions. And their use will only grow. So, I advise the thousands of parents who e-mail us daily and those who review our safety tips online that on how to handle the issue and that they need to be the parent.[3]

Our children are sometimes accessing these sites from their school laptops, in-classroom desktops and school and public libraries. So, a parent's "house rules" may not have much effect when their child leaves the house. So, creating a new law prohibiting schools and libraries from allowing underage students and users to access these sites is an obvious approach. But is the answer to these problems found in laws restricting where students can go during school hours on school computers? Or can this be controlled by blocking access to interactive community networking sites, such as MySpace, Facebook and others from public and school libraries? While this may appear on its face to be an easy answer, it is neither easy nor the answer.

As more social networks are launched every day, and every ISP, entertainment company and wireless provider is either building a social network or finding a way to integrate social networking and community interactivity into their new and existing sites, it is impossible to block all of them and not other valuable Internet features, sites and content. Instead, schools need to be armed with the tools and risk management expertise to decide what sites their students can access during school hours from their servers and how to enforce their decisions and policies.

Schools need to decide if their students should have access to *any* non-educational site from school computers, and if so, which ones and for what purpose. They then need to develop a policy communicating this decision and the rules to the students (in language

[3] See attached advice for parents, in Appendix.

they understand), the teachers, the parents and other caregivers and to their IT team. They need to decide whether they will be using software to help enforce their policy, or merely traditional discipline for violating school policies. That too needs to be communicated to the school community. They also need to create or adopt educational programs teaching their students what information they can and shouldn't be sharing online, the risks of irresponsible Internet use and where to go when things go wrong. They can play an important role in teaching parents and other community members about safe, private and responsible Internet and wireless technologies use.

Educators, not legislators, should be deciding what students do during the school day. They know their students and the learning environment best. But schools do need the guidance and help of legislators and regulators to do this right. They need reliable information and studies on which they can base their decisions. They need to be apprised of new trends and developing risks. They need to know that websites and services are using the latest and best technologies and have adopted the best industry practices with their users' safety in mind. They need help that Congress can provide.

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

Creating a central reporting database where all instances of cybercrimes are reported for statistical purposes, from cyberharassment to Internet-related ID theft, fraud and scams, to sexual predators and Internet-related child pornography and sexual exploitation would be incredibly helpful. It could track cybercrime trends affecting adults, seniors and youth. It could be used to help design safer systems and best practices and guide legislation directed at a meaningful problem, in a meaningful way.

In addition, with tax dollars becoming more and more precious and the mission of all Congressional representatives to put tax dollars into the most effective use, existing programs by trusted non-profit groups can be highlighted and made available online to schools and community organizations that need them, without cost. Without having to reinvent the wheel, massive amounts of programs, lesson plans and risks management guides already exist that can be used as is, or easily retooled. Finding a way to get these wonderful resources into the hands of those who need them the most, using interactive technologies and the Internet and mobilizing volunteers to help deploy existing programs that were developed with or without government dollars is the fastest way to make a dent in the problem. Focusing attention on what works and what doesn't is something that Congress does best. WiredSafety.org and I pledge our help in doing that.

It's time.

Exhibit A: Overview of WiredSafety.org

wired

SAFETY

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

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

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

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

Our target audiences include:

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

Originally formed in 1995 (under another name) to provide help and protection for Internet users of all ages, in recent years, Wiredsafety.org's work has increasingly focused on the safety and good cybercitizenship of children, tweens, and teens. It serves as the umbrella organization for TeenAngels.org, WiredKids.org, WiredCops.org and WiredTeens.org. WiredSafety.org is dedicated to protecting children in cyberspace from cybercrimes and abuse, including from each other. This involves protecting them from cyberbullying, hacking, sexual harassment and identity (ID) theft. It also includes protecting children everywhere from Internet-related sexual exploitation. WiredSafety.org helps protect them from risks posed by adults, by each other and more recently from themselves, as their reputations and future college and job opportunities are impacted by what they post on their MySpace and other profiles. The package of programs designed for young users with the assistance of our teen and preteen volunteers is called "ThinkB4uClick," teaching them the consequences of their cyberactivities.

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

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

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

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

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

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

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

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

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

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

WiredSafety is proud of its reputation as the one-stop-shop for all cyberspace safety, privacy, security, and help needs. It is even prouder of the fact that all this can be accomplished without large government funding or money wasted on administration costs. No one is paid within WiredSafety.org. They are all unpaid volunteers - including Parry herself. This all-volunteer workforce has been estimated at providing more than $3 million in unpaid services every year. Using a popular website and series of special topic sites, the organization has reached millions of Internet users since its inception and addresses more than 5000 children, teens and tweens and 1000 parents in person every month, on average.

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

Exhibit B: Parry Aftab's Bio and CV:

Updated July 2006
Parry Aftab
Bio

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

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

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

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

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

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

Parry Aftab also provides parent Internet education and online safety content for such diverse sites as Nickelodeon, Children’s Television Workshop, Disney, Microsoft, AOL, Yahoo!, Google, AT&T and MSNBC. She is a regular keynote speaker, and resource on camera for the media on diverse cybercrime, safety, privacy and cyberlaw issues. She writes The Privacy Lawyer columnist for Information Week Magazine where she writes on a range of topics that affect technology, policy and privacy. Her expertise is especially in demand on children's Internet issues, because no one knows more about children online than Parry Aftab.

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

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

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

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

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

Parry Aftab

Professional Curriculum Vitae
Phone: 201-463-8663
parry@aftab.com

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

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

---

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

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

SELECT HONORS

Community Leadership Award, 2005
Awarded by Child Abuse Prevention Services

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

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

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

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

ORGANIZATIONS

TRUSTe
Member- Board of Directors (Elected December 2002)

Ad Council
Advisory Committee member (1999 - 2003)

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

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

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

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

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

AUTHORSHIPS AND
RELATED ACTIVITIES

Author, selected books

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

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

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

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

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

Contributor, selected books

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

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

Selected Speaking Engagements

WiredSafety's Social Networking Summit, June 2006

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

National Association of Independent School Annual Conference, March 2006

Stonybrook Cyberbullying Summit, September 2005

FDIC Conference on Security Online, August 2005

The Westchester County Cyberbullying Summit, February 8, 2005

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

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

FTC Workshop on P2P, December 2004

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

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

EU- Safer Internet – Warsaw, March 2004

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

Western Attorneys General Conference, July 29, 2003

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

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

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

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

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

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

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

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

Bertelsmann Foundation, Experts Meeting, Singapore, February 2001

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

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

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

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

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

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

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

APPENDIXES:

Appendix 1:

Parry's Info for Parents...What are our kids doing online?

Know that our kids doing things online that we would freak if we knew about isn't new. Our kids have been saying and doing outrageous things online since the Web was born. We just didn't know about it, but all the other kids do. It's how they communicate online. In 1999 we conducted the largest academic survey done to date for teenage girls. Almost 11,000 of the teens polled answered our questions about what they did online. When we asked them to explain if they had done anything online that they wouldn't have done in person, here's what they said (in their own words):

- "Yes, obviously people are more bold and outgoing on the Internet when they don't have to deal with the consequences of their actions."
- "Of course! All people do. A computer with a phone line is like a mask to the world. You can do or say anything and you won't ever have to meet this person. For instance, my little brother is 13 and he tells people he's 16 or older. He's a sweet guy and has a very high respect for females. Online, however, he says very cruel and suggestive things to and about them. He acts like a monster. It's disgraceful... and a little scary."
- "Yes, of course... our usual boundaries and personal walls are down and we can act more carefree and outspoken if we feel like. At least this is true for me... you can act like a goddess."
- "I have cursed out a lot of ppl [people], and when my bud comes over, we go into places like the African American room and yell "KKK ALL THE WAY" or go to the Jewish room and say "HEIL HITLER," but I haven't done that since I started going back to church and was saved by Jesus Christ. We were just joking, we weren't really racist."
- "Yes, but I'd rather not describe what I did. Instead, I'll just say that online, you can be absolutely ANYONE you want to be, which is why a lot of people do things that they would not normally do. In real life, people everywhere judge you based on your looks, actions, and who knows what else, but online, all that really matters is your attitude and personality."
- "Uh well, I tried cyber sex before and I wouldn't ever do that in real life. Sex period. I don't believe in premarital sex. I think that is a great gift you give your husband. I once told someone off because he/she was being perverted and talking nasty to me and I didn't like it."
- "Well, once I told this guy I met in a chat room all about me and, like, my phone number and stuff. I now realize that this was really stupid of me and will never do anything like it again cause although it's not likely, he could be a psycho or something."
- "I feel I can speak more freely to someone online about my problems because most of them don't go to my school or even the same state. I can ask them advice and they would probably give me the best because they aren't in favor of a certain person. I can introduce myself and meet new people because it isn't as uncomfortable to look into their eyes and if you become really uncomfortable I can just get out of it by blocking them or getting offline."
- "I have had cyber sex... that's something I never have done and never will do until I'm married in real life."
- "I am much more bold online than in real life. I am VERY shy and I say things on the Internet that I normally wouldn't say in public."

- ♦ "I have lied for no reason. Actually, I told a guy I couldn't give him my number cause my mom doesn't want guys calling me cause it was during the school year. My mom doesn't really care who calls me I just didn't know what to say."
- ♦ "Yeah, I wouldn't flirt with people I just met in person, unlike on the Internet."
- ♦ "Flirt more easily, say things I wouldn't say in person, not bad things, just more honest things."
- ♦ "Yeah, because it's a lot easier to talk and get to 'know' someone online because you can't see their face. I never have done anything bad but I've been a lot more easy going and free for what I'd say online then in a live situation which in someways have helped me to be more comfortable talking to new guys in person."
- ♦ "Well, honestly... yes. I had cyber sex! I will never have real sex until I am married, after I engaged in cybering, I totally felt grossed out, like I know I was doing something wrong! I will not make that mistake again."

When we asked them if they ever pretend to be someone else in cyberspace, here's what they answered (in their own words):

- ♦ "Of course I've pretended. Everyone does. You pretend to be older... or you pretend to be a guy... or you just pretend to be whoever you wanna be."
- ♦ "Yes, I just changed myself to be someone I wasn't because I wanted to get a different reaction from people. It gave me a way to see myself as who I wanted to be but by doing it I realized that that is not who I want to be and that I just want to be me."
- ♦ "Yes. If I am ever in a chatroom I always make up things about myself. This is why I say don't trust anyone because everybody else does the same thing."
- ♦ "Since nobody seems to be eager to talk to a 15 year old, I always pretended I was 18 year old female. However, that sometimes attracted bad attention from guys."
- ♦ "Yes. I pretended to be anyone from Leonardo DiCaprio to a serial killer."
- ♦ "I once pretended to be a 16 year old girl. I wanted to talk to my boyfriend to see if he would agree to meet her in person. He did and I told him who I really was and we broke up."
- ♦ "Yes, I've pretended to be so many people. It's fun and safe and because nobody knows who you really are."
- ♦ "Well we've ALL pretended to be older or have a different name or something. Who doesn't? It's part of the fun about being online... you can be whoever you want to be for a little while."
- ♦ "Yes, I pretended to be someone that I wish I could be like a popular person."
- ♦ "I haven't pretended to be someone else, but I have pretended to be a couple of years older than I am, because not many people my age are online to talk to, and if they are, they must be lying about their age, too."
- ♦ "No, I think it is wrong to lie to other people about who you are. I wouldn't want someone to do it to me so I don't do it to them."

When we asked them if they had ever been in a situation online that frightened them, here's what they said:

- ♦ "My friend agreed to meet a guy she met online when he came to our hometown, and she wanted some of us to come along to keep them company. I told my parents but luckily the guy's game got canceled. I wouldn't have gone and I would not support her decision to meet anyone in real life. She kinda felt betrayed but at least she's still alive."
- ♦ "Once I was scared because this guy kept telling me all this stuff about me, like my name, address, friends' names, etc. he said he knew where I lived and stuff,

and I better watch out. It ended up being a joke from a friend of a friend, but I was still scared, and I was very angry at the friend who gave the person the info just to scare me. It wasn't funny."

- "Once I was on ICQ talking to a bunch of my friends when this guy I had been chatting with sent me a file. Unknowingly, I opened it and then I realized that the person had hacked into my system. Suddenly, my CD-ROM drive started opening and closing and annoying (but not threatening) messages started appearing on my screen. Soon after my mouse buttons switched functions. I had just finished a big assignment, so I was afraid the hacker would do something to wreck it. I shut down my computer and that was about all I did about it. One of my friends had a similar experience, only hers was scary and threatening. When she got hacked, pictures of a dead girl with her face smashed in appeared on her screen, along with threatening messages and sound clips."
- "I know this is normal in fact it doesn't bother me I just laugh. Most kids are always exposed to this stuff not just on the Internet so its no big deal in fact sometimes it makes it interesting. But one time this dude got really mad at me and he knew my parents were out of the state and he could have called one of my friends and found my address but instead he kept calling every 5 minutes...."
- "There was one time, when I got online to check my e-mail. I ended up going into my regular chatroom, and when I arrived, some guy started giving out my personal information. I don't know how he knew anything personal about me, but he was telling everyone in there about the frightening and terrible things that were done to me as a child. My best friend doesn't even know what happened to me when I was little. All I did was, denied all of what he said and logged off. I cried all week long."
- "This guy IM'd [instant messaged] me and my best friend and he knew all this information about us... and we hadn't even talked to him before. He knew who we were, where we lived and everything and he kept playing with our minds trying to tell us that we started IMing him first and so on. I told my parents about it but they didn't really care. So this went on for an hour and a half. I had friends try to get him to stop. He told us where he worked and he kept insisting that we go places with him like out to lunch or dinner and he would buy us x-mas and b-day presents even though we had never met him. He would leave them on his car at work for us to come and get, we would go get them and just smash them all over the ground... thinking he would get the point. He was convinced that him and my best friend were dating then I came along and I'm the one who stopped it all. No one could get this guy to stop. We changed our screen names plenty of times but he had already hacked into our account so he could always find us. Well he hacked into mine. Well in December we got a new computer and we both changed our screen names and he hasn't been able to find us since."
- "[A]bout a year ago I met a guy online and I told him my phone # and found out he lived about 5 minutes away from me we talked 4 about a week then he asked me out and I agreed. We met up at the mall he was totally normal 15 year old guy. He wasn't some psycho or anything but I got in a lot of trouble from my parents and I will never give out any personal information again. It's not safe and its a stupid idea. If anyone who reads this is thinking about giving out info to someone on the net PLEASE think twice about it you could get yourself into a lot of trouble."
- "I received a threatening E-mail from someone on my E-mail address. I immediately changed my password, and made sure that I didn't have information on my profile. I never E-mailed the person back, since that is what

lets them know your account is active and they can find out more about you. Then, I decided to make sure about it, and stopped checking my E-mail account. I just got a new one."

- "I was in a chat room once and this person was threatening to kill themselves, and I find that scary. So I IM'd them not to do it, and I chatted with them for a while, and made them feel better about themselves, and promise not to do anything drastic. And they did promise."
- "I told these people to leave this foreign guy alone because they were making fun of him. They were calling him names and mocking everything he said. The people I got smart with told me I better watch my back because they could find out where I lived. That's why I left."

It would be interesting to ask your children to reply to the same questions. You might learn something about your children you didn't know.

Appendix 2:

The Quick Tips on Keeping Our Kids Safe on Social Networks

The quick tips for teens:

- Put everything behind password protected walls, where only friends can see
- Protect your password and make sure you really know who someone is before you allow them onto your friends list
- Blur or morph your photos a bit so they won't be abused by cyberbullies or predators
- Don't post anything your parents, principal or a predator couldn't see
- What you post online stays online - forever!!!! So thinkb4uClick!
- Choose a network that lets you control your own security settings and who can see what you post.
- Don't so or say anything online you wouldn't say offline
- Protect your privacy and your friends' privacy too...get their okay before posting something about them or their pic online
- Check what your friends are posting/saying about you. That cute 14-year old boy may not be cute, may not be 14 and may not be a boy! You never know!

And for parents:

- Talk to your kids
- Don't panic
- Be involved
- This too will pass!

For help or more information, visit WiredSafety.org.

Appendix 3:

Wireless Safety...Keeping Your Kids Safe Using Cellphones and Other Mobile Devices

You've already heard the tips about keeping your kids safe online. But, now...all bets are off. Welcome to the wonderful new world of wireless! Our families can carry powerful computing in handheld devices the size of a pack of playing cards (or smaller!). They can download and play music, movies, and games. They can shoot, store and share photos, video and audio. They are always in touch, always connected, always engaged. (And the newest hottest teen social network, Yfly.com, is using broadcast text-messaging to keep teens connected to their nearest and dearest friends to through their mobile devices too and MySpace and Facebook are using text-to-profile posting technologies now too.)

Great! Except the most often repeated safety tip warns parents to keep the computer in a central location to keep an eye on what's going on. So, how are we supposed to keep our kids safe when they are carrying access and communication devices in the palms of their little hands? Are we supposed to tell them to keep their cell phone or other handheld device in a central location? Of course not. At this point, it's less about standing over their shoulders and more about improving the "filter between their ears."

You can do this by being proactive and informed (not rocket scientists, just informed...). Luckily, it all comes down to 3 key issues. I call these the "3C's" – Communication, Content, and Commercialism. Every digital device or interactive service involves at least one of them, some involve all 3. Once you find the Cs involved, spotting the risks and solutions is easy.

Start by reviewing all your interactive technology devices and services. If you are shopping for a new device or service, ask the salesperson these questions before plunking down your hard-earned money.

- Communication: Does this device or service allow you to communicate with others? Does it allow others to communicate with you? If so, how? What controls exist to block, filter or monitor these communications? How can I implement them? (Text-messaging and voice capabilities fall into the first "C". So do e-mail, interactive features on profiles, and on blogs.)
- Content: What content or images can be accessed or shared using the device or service? Can you surf the Web, access blog or profile sites, post your blog or profile sites or download media? Can you store images, personal information, video, songs, etc? What controls exist to rate, block, filter or monitor the content? How can I implement them? (Music and video downloads, pictures taken by the mobile device, adult content, content on profiles and on blogs fall into this second "C".)
- Commercialism: Can this device/service cost me money? If so, how? Are their ways to spend money or buy things using the device / service? Are their ways to control costs or prevent my kids from spending money or buying things without my approval? What controls exist to block, filter or monitor these costs or spending ability? How can I implement them? (Ringtones, music downloads, text-messaging and games fall into this third C.)

Next, you need to refer to the common sense tips our grandmothers taught our parents and they taught us --we just need to translate them from "Grandma-speak" to "cyberspeak."

Don't talk to strangers.

It's easy for our children to spot an adult in a schoolyard, but not as easy to do the same in cyberspace, or on text-messaging. Our kids need to learn that unless they know the people in real life (“RL”), the person has to be treated like a stranger no matter how long they have chatted online. Period.

Come straight home after school.

When kids wander around, unsupervised, after school they inevitably get into trouble. Allowing your children to spend unlimited time surfing or texting aimlessly is no different. Set a time limit. Create a “no texting” zone, where they spend time with their real life friends and engaging in family activities (and homework).

Don't steal.

Illegal music, movie and game downloads. Enough said!

Don't start fights.

Cyberbullying is when one minor uses interactive technology to harass, frighten or humiliate another minor. They may even spread into RL. Our children should be taught to Stop (don't do anything to make matters worse), Block (the offender) and Tell (you or another trusted adult). (You can learn more about this at stopcyberbullying.org.)

Don’t take candy from strangers.

While we don’t take candy from people online, we do often accept attachments. A seemingly innocent attachment can contain a virus, spyware or a hacking tool. Many of the good anti-virus programs have mobile versions. They are worth the investment.

Don't share personal information with others.

Our children often post their cell number on their instant messaging “away page.” Mobile device cameras can be used to take a picture and post it online. Make sure your children understand what can and cannot be shared. Remember...The more information you give your children, the less information they'll give a stranger.

Look before they leap.

Check things out before your child starts using a new interactive device or technology or activity. Let them know what features you don’t want them using and which ones are safe. And remind them that you will be watching. This is a matter of parental choice and control. The wireless industry is providing some significant help here too. They have voluntarily adopted a set of principles relating to mobile content provided by the carriers themselves, rating them as “restricted” (for those over the age of 18). Restricted content is only available with authentication, allowing parents stay in control. Disney has a new cell phone service and phones launching in June, 2006 too. (Visit disneymobile.com and ctia.org for more information.)

Do unto others as you would have them do unto you.

It is too easy for our children to act out online knowing that they may never have to face the other person in real life. Not having to look them in the eyes makes it easier to be rude, lewd or hostile. This is a good time to remind your children to treat others online and off with R-E-S-P-E-C-T.

Now...go have some fun and play a little! And if you are still tech-challenged, ask your kids for help.

And for more cybersafety tips and help or to book a program for your community, visit WiredSafety.org, the world's largest Internet and wireless safety and help group or contact Parry Aftab directly at parry@wiredsafety.org.

Appendix 4:

Parry's Social Networking Advice for Parents:

It's worth the effort to find out if your child is one of the social networks. Start by asking them. Hopefully they will be honest with you. If they aren't or you suspect they may be lying, it doesn't hurt to check out the more popular ones yourself. Search for your child by e-mail address, name and school. While they often lie about their e-mail address (either creating a special free web-based one just for this, that you may not recognize, or by making one up) or their name, they NEVER lie about their school. That's the only way their friends can find them. If you discover that your child has one of these profiles (or several, which is very common) and is lying to you, you need to take action. This isn't about technology, it's about dishonesty and hiding something important from you. And it might be a good time to buy and install a monitoring product, to be able to find their other lies and their next social-networking website they are trying to keep you from seeing.

If they admit that they have a page and show it to you, review it carefully, without over-reacting. Keep an open mind. (And take 5! To keep from panicking!) Have they posed as someone older? Posted person images? Included their friends on their site or been included by their friends on their sites? Forget the language. It's what kids do online. Caution them, but don't judge them by the language they use online. If they are posting using chatlingo shorthand, you can visit Teenangels.org and use our chatlingo translator to see what they are saying.

Then you have two choices. You can have the site taken down, or you can supervise what they are posting and doing. It's important hat you help keep your child safe online, even if you may be shocked by what you find your child is saying behind your back. And be aware that these are important to them. They all do it, even if they shouldn't. So, it's possible that your young teen will rebel and just set up a page again, but hide it better this time. It may be better to work with them than prohibit the profiles altogether.

Next, don't panic. You should take advantage of this opportunity to review their page first. You might be surprised (hopefully pleasantly) by what they are saying.

If they haven't posted anything to put them at risk, and aren't communicating with strangers, ask them why they want a social-networking profile page. You might be surprised at what they tell you. While parents freak out (understandably) at the provocative images and wild language used by many on these sites, most of the teens don't see them or pay attention to them. They are there to show off their creativity and self-expression and to communicate with their offline friends. As long as they are old enough to understand the rules and adhere to them (no one under 13 is old enough for this, even with parental approval in my humble opinion), and as long as you keep an eye on what they are doing, posting and how they are communicating with others, it's YOUR choice as to whether they keep their site up or not. (Make sure that you don't become the self-appointed profile site, reporting other people's kids for posting underage until you speak with their parents first!)

If you find that they are saying and posting inappropriate things or those comments don't seem to conform to their otherwise good offline behavior, don't panic yet. Think about how our parents would have reacted if they could have seen or heard everything we said to our friends when no adult was around. I guarantee that they would have been almost as shocked as many parents are about what their kids are posting online.

Also, remember that many of the things your kids are saying are being said to impress their audience and are often not true. (Luckily!)

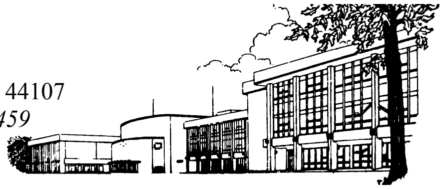
The important difference between what we used to say or do and their posting online, however, is that when we acted out or boasted about acting out, we didn't do it to an audience of millions of people. So, while you shouldn't panic, you should take quick action if your kids are posting personal information in a public forum, or communicating with strangers online.

Now repeat after me..."I am the parent!"

Appendix 5: How schools are handling these issues

A letter for parents from a school, using Parry's tips:

Lakewood High School
14100 Franklin Boulevard   Lakewood, OH 44107
Voice: (216) 529-4028   Fax: (216) 529-4459
Web: http://www.lnoca.org/lakewood/lhs/



Dear Parents/Guardians:

Many of you are aware of the popular websites used by teenagers for blogging and socializing, such as MySpace.com. Recently, our staff has become aware of inappropriate content that many of our students are posting on these public websites. This letter is being sent to inform you of these websites and to encourage you to talk to your child about internet safety and appropriate postings. The following information is provided by Parry Aftab, cyberspace lawyer and executive director of WiredSafety.org, the world's largest Internet safety and help group and taken from her safety tips published at MySpace.com with her permission.

MySpace.com and other similar sites are designed to allow people to share their creativity, pictures, and information with others. Sometimes people do this to find romance. Sometimes they do it to find friends with similar interest. While this may be okay for adults, it is not okay for kids.

MySpace.com recognizes this, and prohibits anyone under 14 years of age from using their website. Unfortunately, while they may set rules to keep younger kids off the site, they can't prevent kids from lying about their age, pretending to be 14 years of age or older. To address this, MySpace.com has developed special software to review the profiles of their members, to try and find anyone under age, based on information the members post about themselves. It's not perfect, but it does help spot many underage members.

While MySpace.com is doing its best to keep your children from using their website and lying about their age, it's up to parents to do their job too. Parents need to talk with their children about not sharing personal information online. Personal information includes pictures, names and addresses, schools they attend, cell and phone numbers and many other less obvious things, such as the name of their school team, ethnic background and even a mall near your house. (You can learn more about how to talk to your kids and what you should be asking at WiredKids.org or WiredSafety.org. I am an Internet privacy and security lawyer and founded the all-volunteer Wired Safety Group. We can help you if things go wrong online, or you just have questions. We provide information, education and one-to-one help for victims of cyberabuse.)

We at WiredSafety.org are developing a special program just for parents concerned about their kids using social-networking and online dating sites. It will teach you what you need to know about finding out if your child has a profile on one of these sites, how to review them and remove them, if you want to. It will also help you if your child is being cyberbullied using one of these sites or members from these sites, or is cyberbullying others.

So what do you, as a parent, do? First you need to find out if your child has a page on one of these sites. The best way to find out if your child has a profile on this or another similar site is to ask them. If you're not sure that your child is being honest with you, you can search MySpace.com (or the other sites) using their e-mail address, or by *searching for their school. (You click on "search" and enter their email address or full name in the appropriate search box.)*

If you find that your child has a profile on the Web site, you should review it. It's amazing how much you can learn about your child by reading their profiles. Does it contain personal information, such as their full name, address or phone numbers? Has your child posted photos? Are they photos of themselves or someone else? Are they sharing poems they write or provocative comments about themselves or others?

If you want the profile removed (you must remove your child's profile if they are under age), first ask your child to remove it themselves. If that doesn't work, MySpace.com has a section explaining how to remove a page. If you find someone who is underage, you can report it there as well. It's not as easy a procedure as the other Web sites.

While MySpace.com is working hard to keep kids off their Web site, ultimately, protecting your child is your job. But you have lots of help. At WiredKids.org and WiredSafety.org thousands of volunteers donate their time to helping parents and children surf responsibly and safely. And we will be building a few tutorials help parents and their children understand how to be careful when communicating publicly online.

A good thing to do is to ask your kids why they created the profile. You might learn that they wanted to share their thoughts with others, make new friends or even allow others in their school to get to know them better. But not all of their motives are as noble or safe. Some may be interested in meeting new romantic interests or role-playing inappropriately online. And when a young preteen lies about their age posing as a seventeen year old at the site, that can be a serious problem. Others in their late teens might approach your child thinking they were older. That's bad for everyone.

If you discover that your child is posting provocative comments or inappropriate images online, it's time for the tough talk. The one about stranger dangers and how that cute fourteen year old boy they meet online may not be cute, may not be fourteen and may not be a boy. (Parents of young boys need to understand that their children are equally at risk. About one-third of the cases of Internet sexual exploitation are men exploiting boys.) Our children need to realize that there are real risks relating to meeting strangers offline, including murder.

It's not easy raising children anymore. It is even harder when the parent is expected to be expert in Internet, cell phone and interactive game risks. The good thing is that you're not facing these challenges alone. We're here to help.

Just remember that while your kids may know more than you do about technology, you know more about life. And you are allowed to set the rules and enforce them. You're still the parent! There is software you can install that will record what your kids say and post online. There is even one that will e-mail you reports at work. The ones I like best are made by Spectorsoft, and can be found at software4parents.com or spectorsoft.com. But don't use them just to spy on your kids. Treat them like a security video camera in the corner of a bank. No one views the tapes unless and until there is a break-in. Do the same here. Check the program reports if something goes wrong. It will collect whatever you need for evidence and to help your child if something goes wrong.

Also, check your parental control programs. Many, such as AOL's and MSN's, can block access to social-networking Web sites or other sites you think are inappropriate for your younger child. There are many other products you can purchase to block sites as well. (Check out software4parents.com to learn about and purchase some of these.) Just remember that the best filter is the one between your children's ears.

Please feel free to contact your child's counselor or house principal if you have any concerns. And visit Parry's cybersafety blog and podcast, http://parryaftab.blogspot.com, and WiredSafety.org for more tips on cybersafety and social networking issues.

A principal's letter to the parents of his students:

I know that history repeats itself and some things never change and there is nothing new under the sun, etc, etc, etc. Having spent so many years in school buildings, I really understand how much truth there is to these clichés. From the first day I started working in schools more than 38 years ago, I have been involved in helping young people deal with the consequences of making poor decisions involving things like drugs, alcohol, vandalism, theft, bullying, etc. It will always be this way and that is part of the job of teachers and administrators in public schools.

It can come as no surprise to anyone reading this that drinking is rampant among many of our students almost every weekend. Drinking to excess (bingeing) is now more common than ever before. Is it watching MTV Spring Break year after year that has caused this new form of excess to be so common? I don't know. I do know that our kids do it, and do it often.

I'm sure everyone knows at some level that to smoke, or snort, or ingest, or inject drugs costs lots of money. How do our kids who choose to engage in this kind of behavior get the money to sustain it? It is either provided to them by way of an allowance or bank card, OR it becomes available in other ways…..theft, sale of personal items, providing services of some kind, etc. We all know enough about drugs either through reading, watching movies, or hearsay, to know that no one provides a sustained supply of drugs to someone else out of the goodness of their hearts. They want something in return. How do our kids get access?

Bullying used to be relegated to the big, tall, tough guy/gal in school. After all, it took muscle and might to back up those words and deeds. Now, through e-mail, instant messages, text messages, the phone, personal home pages, etc. just about anyone can bully someone else and remain anonymous. The 98 pound weakling no longer has to bulk up to be a bully. She/he can do it from the privacy of the bedroom and remain at that weight.

Here is what has really changed. Personal home pages are now almost the norm among our young people with access to computers and broadband Internet service. You would be shocked and surprised to visit some of the home pages of our middle school and high school students. Some of the information they share about themselves is embarrassingly personal, graphic, and explicit, AND it comes with names, addresses, and phone numbers. In truth, most of these kids think they are setting up a page that they and only their close friends have access to. In truth, just about anyone with a real facility with computers can find these sites and pick someone who interests them to prey upon.

I am sharing this disturbing information with you because we all worry about your/our children. Most, if not all of this activity, takes place at home or at someone else's home. If it took place in school, we would have a record and would track it. There are consequences for this kind of behavior at school using school machines and our Internet service. When it happens from elsewhere, we have no control over it. I don't even know how **you** can control it. I simply want the piece of mind knowing that I have shared this with you. It is epidemic among our young people and opens the door for unimaginable problems for them and for YOU, their parents.

I rarely write or speak about problems for which I have few or no solutions. I can't even suggest a solution other than to be vigilant and to know it is going on, if not at your home with your child then with your child's best friend or your neighbor's child. Let's bring this topic into the open and start talking about it whenever groups of adults gather for whatever purpose. Our children need to know that we know what is going on. It is dangerous and they are too young to understand. If you can think of something that would be helpful to parents and you plan on attending the next evening "coffee" in March, please share it with me and I will pass it along to other parents via e-mail or this Newsletter.

Appendix 6:

Parry's Myspace Guidebook Table of Contents
(the guide will be released for back to school without charge at WiredSafety.org)

1- **Introduction to Myspace**
a. Origins/History
b. Why people use it
c. Basic ideas of how Myspace works
d. Explaining the 'cyber friends' process
e. Pitfalls of chatting online
f. Reasons to use social networks

2- **Getting started**
a. Creating your homepage
b. Uploading images/Using appropriate images
c. Content- not revealing too much personal information
d. Settings, and controlling 'Friends' lists
e. Finding others with similar interests, in your area or at your school
f. Using Myspace to network
g. Searching for specific people on Myspace
h. Creating and using an avatar
i. Privacy settings
j. Younger profiles settings (between 14 and 16)
k. Reporting abuse
l. Getting help
m. Pics, quizzes and getting codes from third party sites

3- Writing a profile
a. Creativity-expressing yourself through a blog/profile
b. Blog/profile ideas, like a diary, it can be a journal of your thoughts
c. Writing with some caution-not revealing detailed information
d. Reading and contributing to other members blogs/profiles

4- Hazards of meeting people from the Internet in real life
a. Using caution when replying to e-mails and communications from strangers
b. Unsolicited contact, using judgment to better safeguard yourself
c. Meeting people face to face offline
d. "You never know..." how even smart teens and preteens are tricked by posers
e. You don't have to meet them offline to be sexually exploited - webcams, cybering and child pornography

5- Risks from adults, from other teens and risks you pose to yourself
a. Sexual exploitation issues
b. Cyberbullying, stalking and harassment
c. Protecting your reputation online
d. What employers, colleges and police are doing on social networks
e. ID theft, scams and posing
f. Protecting your passwords and personal information
g. Protecting your personal information - when your friends post your info

6- What you need to know to keep yourself safer
a. Having fun on Myspace, safely

b. Using good judgment to identify potential dangers
c. Using creativity to express yourself through blogs/profiles
d. Letting an adult know if something happens
e. Talking to parents/adults about people you meet online
f. Using extra caution when sharing images or chatting
g. Talking to friends about safety - protecting yourself and your friends online

Appendix 7:

Parry Aftab's Guide to Keeping Your Kids Safe Online

MySpace, Facebook and Xanga, Oh! My!

Keeping yourself and your kids safe on social networks

The quick tips for teens:

- Put everything behind password protected walls, where only friends can see
- Protect your password and make sure you really know who someone is before you allow them onto your friends list
- Blur or morph your photos a bit so they won't be abused by cyberbullies or predators
- Don't post anything your parents, principal or a predator couldn't see
- What you post online stays online - forever!!!! So thinkb4uClick!
- Don't so or say anything online you wouldn't say offline
- Protect your privacy and your friends' privacy too...get their okay before posting something about them or their pic online
- Check what your friends are posting/saying about you. Even if you are careful, they may not be and may be putting you at risk.
- That cute 14-year old boy may not be cute, may not be 14 and may not be a boy! You never know!
- And, unless you're prepared to attach your MySpace to your college/job/internship/scholarship or sports team application…don't post it publicly!

And for parents:

- Talk to your kids – ask questions (and then confirm to make sure they are telling you the truth!)
- Ask to see their profile page (for the first time)…tomorrow! (It gives them a chance to remove everything that isn't appropriate or safe…and it becomes a way to teach them what not to post instead of being a gotcha moment! Think of it as the loud announcement before walking downstairs to a teen party you're hosting.)
- Don't panic…there are ways of keeping your kids safe online. It's easier than you think!
- Be involved and work with others in your community. (Think about joining WiredSafety.org and help create a local cyber-neighborhood watch program in your community.)
- Remember what you did that your parents would have killed you had they known, when you were fifteen.
- This too will pass! Most kids really do use social networks just to communicate with their friends. Take a breath, gather your thoughts and get help when you need it. (You can reach out to WiredSafety.org.)
- It's not an invasion of their privacy if strangers can see it. There is a difference between reading their paper diary that is tucked away in their sock

drawer…and reading their MySpace. One is between them and the paper it's written on; the other between them and 700 million people online!

- Don't believe everything you read online – especially if your teens posts it on her MySpace!
- And, finally….repeat after me – "I'm still the parent!" If they don't listen or follow your rules, unplug the computer…the walk to the library will do them good. ☺

For more information, visit WiredSafety.org. Copyright Parry Aftab 2006, all rights reserved. For permission to duplicate, e-mail Parry@WiredSafety.org.

Appendix 8:

SNAPSHOT OF U.S. MINORS ONLINE AND HOW PREDATORS REACH THEM
(Taken from Parry Aftab's testimony before the House Sub-Committee on Investigations and Oversight on April 4, 2006)

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

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

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

Putting Their Heads into the Lion's Mouth

Now, I will share something very controversial. While educators and child psychologists understand this, most parents will be shocked at the suggestion that their preteens and teens are in control of their safety online and putting themselves at risk, often intentionally. But unless we accept this, and direct our attentions at solutions aimed at this reality, we are all wasting our time. We will focus on the much smaller segments of preteens and teens who are being victimized through not fault of their own - those who are targeted at random. All others need to change their online behaviors. And that's where we need to devote all our attentions.

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

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

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

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

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

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

Preteens and Teens at Risk: Most of the high risk preteens and teens fall into three categories: those who are naive and looking for love and affection (typically the "loners" and "shy" preteens and teens), those who already engage in other high risks activities, such as drug and alcohol abuse, driving too fast or doing risky things for the thrill of it (often the student leaders, athletes, cheerleaders and very competitive teens, the risks takers and thrill seekers looking to let off steam or impress their peers) and those who don't realize that what they do online is real, the ones who are looking to appear older, cooler, more fun and more popular (most of the teens and especially preteens fall into this category at least once). Sadly, most of our preteens and teens fit one of these categories. Sadder still is the fact that in recent years we have learned that most preteens and teens are potential victims.

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

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

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

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

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

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

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

The Anatomy of a Cyberpredator:

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

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

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

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

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

Some cyberpredators (known as "travelers" to law enforcement) seek out the good kids, the smart ones, the ones who are not street-smart and are from sheltered suburban or rural families. Many of our children match that profile perfectly. Others, however, target (or are targeted by) popular, super achiever, risk preferring teens. It took the death of a young teen from Connecticut, Christina Long, before we realized that many of the incidents involved teens who did not fit the loner profile. What we learned was that these kids never report any attacks or exploitation. The only time we hear of these cases is when the teen is kidnapped or killed.

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

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

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

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

Saturday arrives, and the child goes to the mall and meets an adult outside the computer game store. He identifies himself as "Uncle George" and explains that his nephew is already at the McDonald's waiting for them. The child is uncomfortable, but the uncle walks into the store and buys the $100 game. He comes out and hands it to the child, who is immediately neutralized and delighted. Stranger-danger warnings are not applicable. This isn't a stranger—he's "Uncle George," and if any proof was needed, the computer game is it. He gets into Uncle George's car without hesitation to meet his friend at McDonald's. The rest is reported on the 6 o'clock news.

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

The Script—How They Operate Online

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

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

Why It Works

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

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

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

This atmosphere does two things: It creates a distance between the child and her parents, at the same time bringing the child into a special secret alliance with the pedophile. (You should know that boys are almost as often the victims of Internet sexual exploitation as girls are, but they report it less frequently.)

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

Anatomy of a Real and Early Case

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

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

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

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

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

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

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

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

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

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

Getting in Under Your Radar:

Even when parents are watching, bad things can happen.

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

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

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

Jennifer's mother, Sharry (also not her real name), talked to Jennifer about her online friend, Charlie. She insisted on talking to Charlie himself, by phone, once he and Jennifer had started calling each other. He passed the phone call test, and Sharry was convinced that he really was the teenage boy he professed to be. Either he had manipulated his voice to sound younger or he had a younger person make the call. Charlie even called and spoke to Jennifer's brothers, talking about when he would be their brother-in-law someday, after he and Jennifer were married. He pleaded with Jennifer to come and visit him in Utah. Sharry invited him to visit them instead. But Charlie always had a reason he couldn't come.

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

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

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

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

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

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

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

Using Celebrity's Names

I was having lunch in Los Angeles with one of my girlfriends when Nick Lachey walked into the restaurant. She pointed him out to me and I immediately grabbed my business card and approached his table (to the utter embarrassment of my friend). I introduced myself and told him I needed his help. I explained that predators were using his name and the name of other celebrities to lure kids into meetings and unsafe activities. They find teens who post their favorite celebrities on their profiles, websites or other online communications. Then they create a profile claiming to be a close personal friend of that celebrity. They offer to forward a pic of the teen to the celebrity, and seek sexier and sexier pics as time goes on, ultimately ending with an offer to introduce the teen to their favorite celebrity in real life. Years ago, Justin Timberlake was the most popular of these celebrity lures. Nick is now. He listened intently and turned white when he realized people where using his name to hurt his young fans. He offered his help.

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

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

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

[Appendixes omitted]

Appendix 9: Parenting Online

wired SAFETY

Parenting Online

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

CyberSense
...translating common sense for cyberspace

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

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

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

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

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

there could be strangers lurking and reading your posts without letting you know that they are there. Don't let your children put personal information on profiles. It's like writing your personal diary on a billboard.

With children especially, sharing personal information puts them at risk. Make sure your children understand what you consider personal information, and agree to keep it confidential online and everywhere else. Also teach them not to give away information at Web sites, in order to register or enter a contest, unless they ask your permission first. And, before you give your permission, make sure you have read the web site's privacy policy, and that they have agreed to treat your personal information, and your child's, responsibly.

- **We need to get to know your friends.** Get to know their online friends, just as you would get to know their friends in everyday life. Talk to your children about where they go online, and who they talk to.
- **R-E-S-P-E-C-T.** We all know the golden rule. We have a special one for cyberspace. Don’t do anything online you wouldn’t do offline. If you teach your child to respect others online and to follow the rules of netiquette they are less likely to be cyberbullied, become involved in online harassment or be hacked online. You can learn more about the ways to combat cyberbullying at our new website, StopCyberbullying.org or at WiredSafety.org’s cyberstalking and harassment section. Remember that it is just as likely that your child is a cyberbully (sometimes by accident) as a victim of one. Let them know they can trust you not to make matters worse. You have to be the one they come to when bad things happen. Be worthy of that trust.

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

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

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

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

What Tech Tools Are Out There?

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

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

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

Blocking Software

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

Filtering

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

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

Outgoing Filtering

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

Monitoring and Tracking

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

We particularly recommend using a monitoring software and then forgetting it's installed. Think of it as the security video camera in the corner of the bank. No one views the tapes until the bank is robbed. If something bad happens, you can play back the monitoring log and see exactly what occurred, and who said what, and in dire situations, where your child went to meet an adult offline. We particularly like Spectorsoft.com, because their products can monitor all instant messaging platforms, which is key to keeping your children safe online.

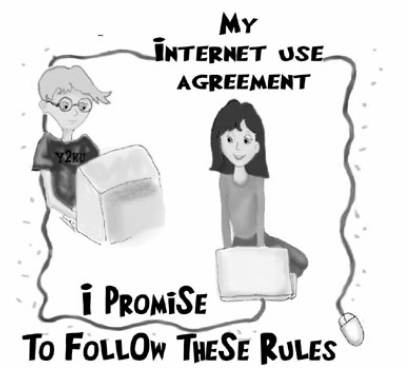
Parents have to remember, though, that these tools are not cyber-babysitters. They are just another safety tool, like a seat belt or child safety caps. They are not a substitute for good parenting. You have to teach your children to be aware and careful in cyberspace. Even if you use every technology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

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

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

PARENTING ONLINE

MY AGREEMENT ABOUT USING THE INTERNET



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

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

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

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

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

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

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

From Parry:

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

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

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

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

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

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

Remember, we're all in this together!

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

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

MR. UPTON. Ms. Collins.

MS. COLLINS. Mr. Chairman and distinguished members of the committee, I welcome this opportunity to appear before you to discuss these issues. Chairman Upton, you have a demonstrated record of commitment to child protection. I commend you and your colleagues for your leadership initiative. The National Center for Missing and Exploited Children joins you in your concern for the safety of the most vulnerable members of our society. Let me first provide you with the background information.

We are 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.

One of the programs that we operate that I am responsible for is the CyberTipline. It is the 9-1-1 of the Internet, which serves as the Nation's clearinghouse for investigative leads and tips regarding crimes against children, both online and off.

The leads are reviewed by the analyst in the Exploited Child Unit of NCMEC, who visit the website, examine and evaluate the content, use search tools to identify the perpetrators, and provide all of the information to the appropriate law enforcement agency. The results: In 8 years since the Cyber site began, we received over 400,000 leads. We average about 1,500 a week at this point.

Despite our progress, the victimization of children continues and there is evidence that it is increasing. The number of reports on online enticement of children to the CyberTipline has increased 400 percent since 1992. Our records are showing that there is a significant and steady increase in the reports of online entities.

Recently there has been great attention to the Social networking websites. While they are used by adults, kids are finding them attractive and there have been incidents, as has been mentioned earlier, where predators have taken advantage of the information that the kids have presented about themselves. And the information they are putting onto these networking sites do make them vulnerable.

At this point we are receiving approximately 250 reports of entities each week, and those are just people who know to report to the CyberTipline.

Last month, we hosted a dialogue of social networks sites here in Washington, D.C. It was a day-long series of panels, audience discussion on the popularity of social networking sites as well as the misuse of technology. The panelists included leaders from the technology industries, policymakers, law enforcement, child advocacy groups. The attendees were able to question representatives from MySpace, Facebook, and Xanga, the FBI's Innocent Images Unit, two Internet Crimes Against Children Task Force investigators, age verification and digital imaging analysis experts, the Internet Education Foundation, Net Family News, the Pew Foundation, and two State attorneys general.

It was a vigorous and informative exchange, but what did we learn? We learned that social networking sites tapped into the lives of teenagers to exploit themselves. We learned that the operator of social networking sites don't want the customers to be endangered by their sites, but state they want to remain competitive in the booming market. We have learned that more restrictions could cause teens to go somewhere else that has fewer restrictions, but have the unintended consequences of increasing their chances of being victimized. We have learned that the current age verification technology is ineffective for children too young to appear in a public record database. We learned the increased importance of education messages and engaging teens to become a part of their own online safety. We learned they can work together to solve this problem with the help of policymakers, law enforcement, and child advocacy groups.

The recent concern about social networking sites has given the operators of these sites a clear window of opportunity to take this problem seriously and take action to make their sites safer for children. NCMEC is encouraged by the steps already taken by some of these sites. MySpace has named a new chief security officer, a former Federal prosecutor with experience in child exploitation issues. And other sites have demonstrated a similar commitment and are in the process of changing certain features in the architecture of their sites to make children safer.

These are important first steps, but we strongly encourage the social networking companies to continue their progress by working closely with the various State attorneys general, law enforcement, and others to bring about real change. There is more that can be done and it must be done now.

We need to do a better job, as a Nation, of identifying and addressing the greater risk to our children today. We need to help protect children through education, open dialogue, and elevated awareness. By working with industry leaders, we can expand our outreach, educate parents, guardians, and teens and the general public about social network sites and ensure safer ways for them to be online.

MR. UPTON. Thank you.

[The prepared statement of Michelle Collins follows:]

PREPARED STATEMENT OF MICHELLE COLLINS, DIRECTOR, EXPLOITED CHILD UNIT, NATIONAL CENTER FOR MISSING AND EXPLOITED CHILDREN

Mr. Chairman and distinguished members of the Committee, I welcome this opportunity to appear before you to discuss social networking websites and the use of the Internet to victimize children. Chairman Upton, you have a demonstrated record of commitment to child protection and I commend you and your colleagues for your leadership and initiative. The National Center for Missing & Exploited Children ("NCMEC") joins you in your concern for the safety of the most vulnerable members of our society and thanks you for bringing attention to this serious problem facing America's communities.

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

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

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

This last category was added as a result of enactment of the PROTECT Act in 2003.

These leads are reviewed by NCMEC analysts, who visit the reported sites, examine and evaluate the content, use search tools to try to identify perpetrators, and provide all lead information to the appropriate law enforcement agency. The FBI, ICE and Postal Inspection Service have "real time" access to the leads, and all three agencies assign agents and analysts to work directly out of NCMEC and review the reports. The results: in the 8 years since the CyberTipline began operation, NCMEC has received and processed more than 400,000 leads, resulting in hundreds of arrests and successful prosecutions.

However, despite our progress the victimization of children continues and there is evidence that it is increasing. The number of reports of online enticement of children to the CyberTipline increased 400 percent since 1998. Our records show a significant and steady increase in these reports over the years. This upward trend is very disturbing and shows the seriousness of this issue. But this is not the only evidence.

It has been established that youth who use the Internet regularly receive sexual solicitations over the Internet. However, very few of these sexual solicitations are reported to authorities. This clearly demonstrates that children are at risk and that we must do more.

Over the years as technology has evolved so, too, have the methods for victimizing children. The Internet has provided a veil of apparent anonymity, enabling predators to seek out children, win their confidence and then victimize them.

As technology evolves, so does the creativity of the predator. Today, we are hearing a great deal about new innovations, including the use of webcams, social networking websites and Internet access on cell phones.

These innovations are popular and are utilized by millions of Americans. Yet, as with every other new program or service, there are those who would use them inappropriately and for unlawful purposes.

Recently there has been great attention to the social networking websites. While they are used by adults, kids are enormously attracted to them, and there have been instances in which offenders have taken advantage of the images and information displayed to target kids. The unprecedented amount of personal information that teens are posting to social networking websites makes them vulnerable to people who want to harm them.

Some of the social networking sites link defined communities of registered users, such as students attending a particular college or high school. Others are open to anyone over a certain age. These websites permit registered users to create an online profile, including photographs, with categories of interest such as music and sports, as well as an online journal. They are highly personalized and often extremely detailed. Children consider this to be an easy way to connect with friends, find new friends and share their thoughts and feelings. The teenage years are a time of personal exploration. This is only natural. However, the new form of social interaction is over the Internet, exposing children to, literally, a world of potential danger.

Child predators consider these sites to be an easy way to find child victims. They can use the information posted by children to forge a ‘cyber-relationship’ that can lead to that child being victimized. The number of reports to our CyberTipline involving social networking sites has increased. In recent years, many kids were using their email profiles and chat rooms in a similar fashion to share their hobbies and interests and make “friends.” However, those forums didn’t have nearly the same implications as the social networking sites, with their enormous universe of users.

Last month, NCMEC hosted a Dialogue on Social Networking Sites here in Washington, D.C. It was a day-long series of panelist-audience discussions on the popularity and misuse of this technology and ways to help keep children safer while using them. The panelists included leaders from the technology industry, policy makers, law enforcement, academia and children’s advocacy groups. The attendees questioned representatives from the social networking sites Myspace, Facebook, and Xanga, the FBI’s Innocent Images Unit, two Internet Crimes Against Children Task Force investigators, age verification and digital imaging analysis experts, the Internet Education Foundation, Net Family News, the Pew Foundation and two state attorneys general.

It was a vigorous and informative exchange.

What did we learn?

We learned that social networking sites tap directly into the needs of teenagers to define themselves, explore their own creativity and reach out to their peers. We learned that operators of social networking site don’t want their customers to be endangered by their sites but at the same time want to remain competitive in this booming market. We learned that more restrictions will cause teens to go somewhere else that has fewer restrictions, with the unintended consequence of increasing their chances of being victimized. We learned that the current age verification technology is ineffective for children too young to appear in public records databases. We learned the increased importance of education messages, and engaging teens to become a part of their own online safety.

We learned that the industry's brightest minds that created this technology in the first place can work together to solve this problem, with the help of policy makers, law enforcement and children's advocacy groups.

The recent concern about social networking sites has given the operators of these sites a clear window of opportunity to take this problem seriously and take action to make their sites safer for children. NCMEC is encouraged by the steps already taken by some of these sites. Myspace has named a new Chief Security Officer, a former federal prosecutor with experience in child exploitation issues. Other sites have demonstrated a similar commitment, and are in the process of changing certain features on their sites that help make children less vulnerable.

These are important first steps, but we strongly urge them to continue their progress by working closely with the various state Attorneys General, law enforcement and others to bring about real change. There is more that can be done and the time to do it is now.

We need to do a better job as a nation of identifying and addressing the greatest risks to our children today. We need to help protect children through education, open dialogue and elevated awareness. By working with industry leaders we can expand our outreach and educate parents, guardians, teens and the general public about this recent technology and ways to ensure safer experiences online.

Thank you.

MR. UPTON. Mr. Davis.

MR. DAVIS. Thank you, Chairman Upton and Members of the Subcommittee, for this opportunity to testify on Deleting the Online Predators Act of 2006. I have to tell you, I have already learned a lot this morning just from the testimony I have heard so far.

My name is Ted Davis, and I am an Information Technology Director with the Fairfax County Public Schools in Virginia. FCPS is the 14th largest school district in the United States, with over 163,000 students at 228 schools. FCPS has long since recognized the promise of the Internet as an educational resource as well as its perils. Thus in 1997, I was tasked with leading the effort to develop our Internet use policy and to implement filtering technology.

FCPS supports the goals of the legislation but opposes the legislation in its current form. As I will elaborate, public schools are addressing the dangers of online predators. Legislation would not substantially improve the safety of our students and would place an added burden on schools.

Based on input gathered from nearly 800 educators, we recognize that technology alone could not address our shared concerns for the safety of our students. Thus in 1998, the Fairfax County School Board adopted a policy that emphasized education, classroom management, personal responsibility, as well as technology.

Two years prior to the Children's Internet Protection Act of 2000, FCPS implemented a filtering technology now known as Symantec Web Security. FCPS filters Web content that is obscene, harmful to juveniles, child pornography, and promotes illegal activities. Today all 90,000-plus of our computers are filtered for such consent.

SWS enables school districts to select from a wide range of categories of inappropriate materials for filtering, such as sex, crime, violence, intolerance, and interactive chat. So the districts may select materials to be blocked based on their policies.

As you know, the Internet is constantly changing. Thus, filtering vendors like Symantec continually update their lists of inappropriate websites in these categories. Filtering vendors use a combination of technology and human review to identify and classify inappropriate websites.

Furthermore, SWS provides school districts to block or unblock additional sites in accordance with the needs of the school system. FCPS put into place a process and guidelines for identifying and evaluating websites for possible filtering. Social sites like MySpace fail under this process. In the case of MySpace, FCPS began blocking this site last November. The same is true for many sites that predated MySpace.com. A neighboring school district took similar action.

As you might expect, there will always be some determined students that seek to bypass technology protection measures. These students are subject to policy enforcement. Each school year, FCPS students are required to sign our acceptable use policy which outlines appropriate and inappropriate use of computers and the Internet. Failure to comply with this policy results in disciplinary action.

Fortunately, this is not a significant problem. In this past school year, 578 students were disciplined for violating our acceptable use policy. This represents 0.3 percent of our student population. One strategy for deterring AUP infractions is through good classroom management. That is how teachers make use of their Internet in their classrooms: arranging computers so that screens are visible to a teacher, preselecting websites for instruction, walking the classroom, and interacting with students as they use the Web.

The teachers are trained to use these practices, to work them into their routine. Technology measures, policy enforcement, and classroom management are good strategies for preventing access to inappropriate materials in school, but they do not sufficiently prepare our students to deal with potential dangers outside of school, at home, a friend’s house, a coffee shop or even when they become adults. We know that our students will need to deal with many dangers, not only sexual predators but also identity thieves, scams, phishing scams, viruses, deceptive advertising, and misinformation.

Education is the key to preparing our students to deal with these dangers.

That is why FCPS began at the earliest age to teach students how to take advantage of the Internet and to deal with its dangers. We teach them not to give out personal information, that people may not be who they say they are, and never agree to meet someone via the Internet. To make our point, we also partner with the Fairfax County Police who can speak to our students of these dangers from real experience.

Parents are also key to protecting and educating their children. To help parents, we conduct senior safety nights to educate them on the benefits and dangers. We teach parents to get involved in their children's Internet use at an early age, to set rules on Internet use, and to place computers in the common areas of the home. We also reach out to businesses and parents via brochures and videos.

The strategies I described, taken together, have been effective in FCPS for many years now. These are not the direct result of State or Federal legislation; rather, they are the result of the close relationship our schools enjoy with our students, parents, and community and our shared passion to provide a safe learning experience.

Nevertheless, since the passage of the Children's Protection Act 6 years ago, these strategies are now commonplace in schools throughout the country.

The proposed legislation, though an extension of similar provisions in effect today, does not lend itself to a technical solution. It would require that schools block commercial social networking sites that may easily be misused to perpetrate inappropriate contact with students. Unlike current restrictions against obscene materials that can be objectively identified, this legislation requires schools to subjectively protect which sites may be misused. Identifying and evaluating such sites would not take advantage of the technical capabilities of filtering vendors and likely lead to blocking of legitimate instructional cites. Thus this burden would fall back on to the schools.

More could be done, of course. You could help protect our students by pursuing those individuals who would do harm to our children. And you can help us educate and prepare our students to be safe citizens of the Internet. To these ends you could support law enforcement activities that seek to apprehend perpetrators before they harm a child.

I like the concept of the CyberTipline. You can facilitate collaboration between law enforcement agency, filtering vendors, and schools to share information on websites used to commit crimes, such as that proposed by the Federal Trade Commission, and you can foster an information campaign to reach parents and students on how to face the dangers on the Internet. A novel approach here would be to require social networking sites to commit some of their prominent advertising space to public service announcements. That way, those who profit from these sites will bear some of those costs.

Thank you again for this opportunity to speak before the committee. I welcome your questions.

[The prepared statement of Ted Davis follows:]

PREPARED STATEMENT OF TED DAVIS, DIRECTOR, KNOWLEDGE ASSET MANAGEMENT, IT DEPARTMENT, FAIRFAX COUNTY PUBLIC SCHOOLS

Background:

- Ted Davis is an information technology director at Fairfax County Public Schools (FCPS) that led the development of the FCPS Internet use policy and filtering technology implementation.
- FCPS is the 14th largest public school district in the United States.
- FCPS supports the goals of the legislation, but opposes the legislation as written.

Protecting students on the Internet at FCPS:

- Internet use policy emphasizes education, classroom management, personal responsibility, as well as technology.
- Implemented the Symantec Web Security (SWS) product in 1998.
- Filters content based on pre-selected SWS categories.
- Established a process for filtering additional web sites.
- Began blocking MySpace.com in November, 2005.
- Enforces an Acceptable Use Policy to deter inappropriate behaviors.
- Performs classroom management activities to mitigate infractions of its policies.
- Technology measures, policy enforcement, and classroom management do not prevent inappropriate behaviors outside of the school.
- Education of students and parents is key to preparing children to deal with dangers on the Internet.

Legislation:

- The proposal to block social networking sites that “may easily be” misused does not lend itself to a technical solution.
- Identifying sites that may be misused is subjective and would place an added burden on schools.
- The Subcommittee could help schools by:
    - Supporting law enforcement in identifying and apprehending predators.
    - Facilitating collaboration between law enforcement agencies, filtering vendors, and schools in identifying web sites used to commit crimes.
    - Fostering an information campaign to reach parents and students on how to face dangers on the Internet.

Thank you Chairman Upton and members of the Subcommittee for this opportunity to testify on the Deleting Online Predators Act of 2006.

My name is Ted Davis and I am an information technology director with Fairfax County Public Schools (FCPS) in Virginia. FCPS is the 14th largest public school district in the United States with over 163,000 students at 228 schools. FCPS long ago recognized the promise of the Internet as an educational resource, as well as its perils. Thus, in 1997, I was tasked with leading the effort to develop our Internet use policy and to implement filtering technology. FCPS supports the goals of the proposed legislation, but opposes the legislation in its current form. As I will elaborate, public schools are addressing the dangers of online predators, the legislation would not substantially improve the safety of our students, and it will place an added burden on schools.

Based on input gathered from nearly 800 educators, students, parents, and community members, we recognized that technology alone could not address our shared concerns for the safety of our students. Thus in 1998 the Fairfax County School Board adopted a policy that emphasized education, classroom management, personal responsibility, as well as technology.

Two years prior to the Children's Internet Protection Act of 2000, FCPS implemented a filtering technology now known as Symantec Web Security (SWS). FCPS filters web content that is obscene, harmful to juveniles, child pornography, and promotes illegal activities. Today, all 90,000+ of our computers are filtered for such content.

SWS enables school districts to select from a wide range of categories of inappropriate materials for filtering, such as sex, crime, violence, intolerance, and interactive chat, so that districts may select materials to be blocked based on their policies. As you know, the Internet is constantly changing, thus filtering vendors, like Symantec, continually update their lists of inappropriate web sites in these categories. Filtering vendors use a combination of technology and human review to identify and classify inappropriate web sites.

Furthermore, SWS provides school districts the ability to block (or unblock) additional sites in accordance with the needs of the school system. FCPS put into place a process and guidelines for identifying and evaluating web sites for possible filtering. Social sites, like MySpace.com, fell under this process. In the case of MySpace.com, FCPS began blocking this site last November. The same is true for many sites that preceded the popularity of MySpace.com. Neighboring school districts took similar actions—much to the relief of parents and dismay of students.

As you might expect, there will always be some determined students that seek to bypass technology protection measures—these students are subject to policy enforcement. Each school year FCPS students and their parents are required to sign our Acceptable Use Policy, which outlines appropriate and inappropriate uses of computers and the Internet. Failure to comply with this policy results in disciplinary action. Fortunately, this is not a significant problem. In this past school year 578 students were disciplined for violating our Acceptable Use Policy—representing 0.3% of our student population.

One strategy for deterring AUP infractions is through good classroom management. That is how teachers make use of the Internet in their classrooms. This includes approaches such as arranging computers so that screens are visible to the teacher, pre-selecting web sites for instruction, walking the classroom, and interacting with students as they use the web. FCPS teachers are trained to work these practices into their technology routine.

Technology measures, policy enforcement, and classroom management are good strategies for preventing access to inappropriate materials in school, but they do not sufficiently prepare our students to deal with potential dangers outside of school—at home, a friend's house, a coffee shop—or even when they become adults. We know that our students will need to deal with many dangers—not only sexual predators, but also identity thieves, scams, phishing schemes, viruses, deceptive advertising, and misinformation. Education is the key to preparing our students to deal with these dangers.

That is why FCPS begins at the earliest age to teach students how to take advantage of the Internet and to deal with its dangers. We teach them not to give out personal information, that people may not be who they say they are, and never to agree to meet someone via the Internet. To make our point, we also partner with the Fairfax County Police who can speak to our students of these dangers from real experience.

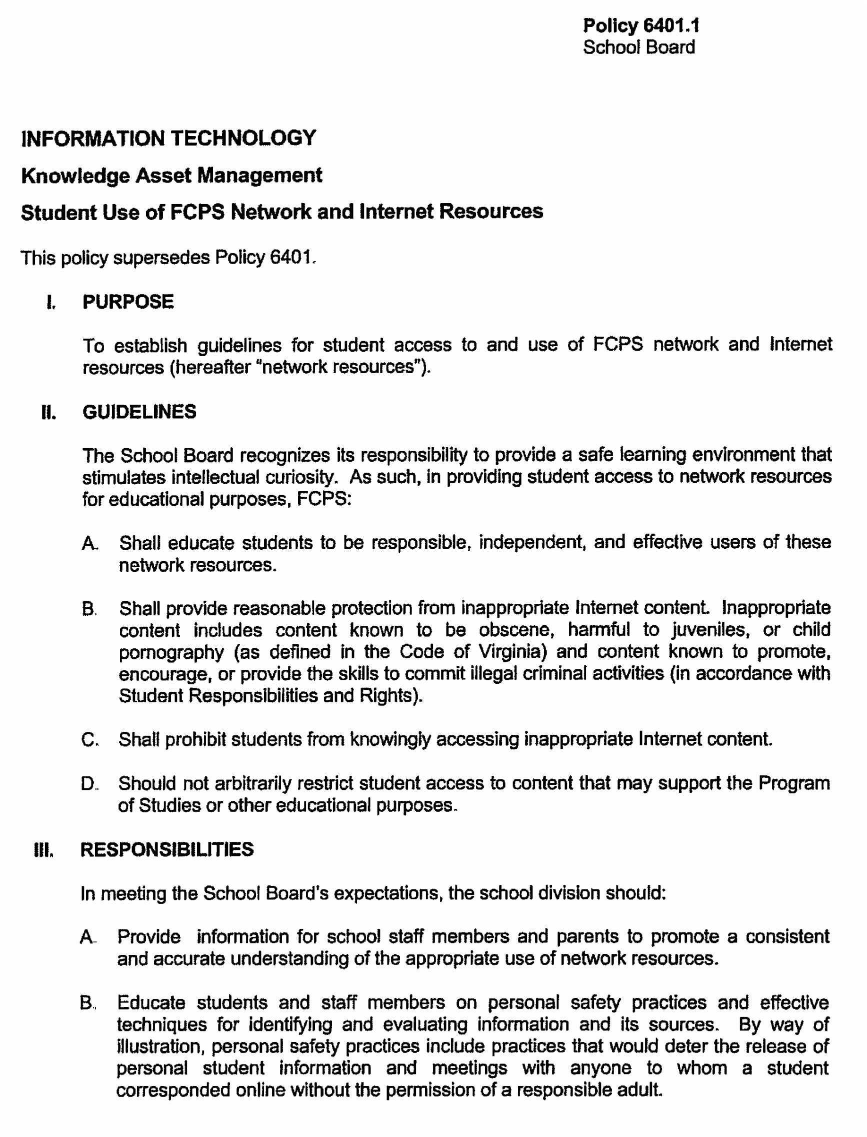
Parents are also key to protecting and educating their children. To help parents, we conduct cyber safety nights to educate them on the benefits and dangers. We teach parents to get involved in their children's Internet use at an early age, to set rules on Internet use, and to place computers with Internet access in a common area of their homes. We also reach out to busy parents via brochures and videos.

The strategies I described, taken together, have been effective in FCPS for many years now. These strategies are not the direct result of state or federal legislation. Rather, they are the result of the close relationship our schools enjoy with our students, parents, and community—and our shared passion to provide a safe learning experience that meets our students' needs. Nevertheless, since the passage of the Children's Internet Protection Act six years ago, these strategies are now commonplace in school districts throughout the country.

The proposed legislation, though an extension of similar provisions in effect today, does not lend itself to a technical solution. It would require that schools block commercial social networking sites that “may easily be” misused to perpetrate inappropriate contact with students. Unlike current restrictions against obscene materials that can be objectively identified, this legislation would require schools to subjectively predict which sites may be misused. Identifying and evaluating such sites would not take advantage of the technical capabilities of filtering vendors and likely lead to blocking of legitimate instructional sites. Thus this burden would fall back on to the schools.

More could be done, of course. You can help protect our students by pursuing those individuals who would do harm to our children, and you can help us educate and prepare our students to be safe citizens of the Internet. To these ends, you could support law enforcement activities that seek to apprehend predators before they harm a child. You can facilitate collaboration between law enforcement agencies, filtering vendors, and schools to share information on web sites used to commit crimes; and you could foster an information campaign to reach parents and students on how to face the dangers on the Internet.

Thank you again for this opportunity to speak before the committee. I welcome your questions.



Policy 6401.1
School Board

INFORMATION TECHNOLOGY

Knowledge Asset Management

Student Use of FCPS Network and Internet Resources

This policy supersedes Policy 6401.

I. **PURPOSE**

To establish guidelines for student access to and use of FCPS network and Internet resources (hereafter "network resources").

II. **GUIDELINES**

The School Board recognizes its responsibility to provide a safe learning environment that stimulates intellectual curiosity. As such, in providing student access to network resources for educational purposes, FCPS:

A. Shall educate students to be responsible, independent, and effective users of these network resources.

B. Shall provide reasonable protection from inappropriate Internet content. Inappropriate content includes content known to be obscene, harmful to juveniles, or child pornography (as defined in the Code of Virginia) and content known to promote, encourage, or provide the skills to commit illegal criminal activities (in accordance with Student Responsibilities and Rights).

C. Shall prohibit students from knowingly accessing inappropriate Internet content.

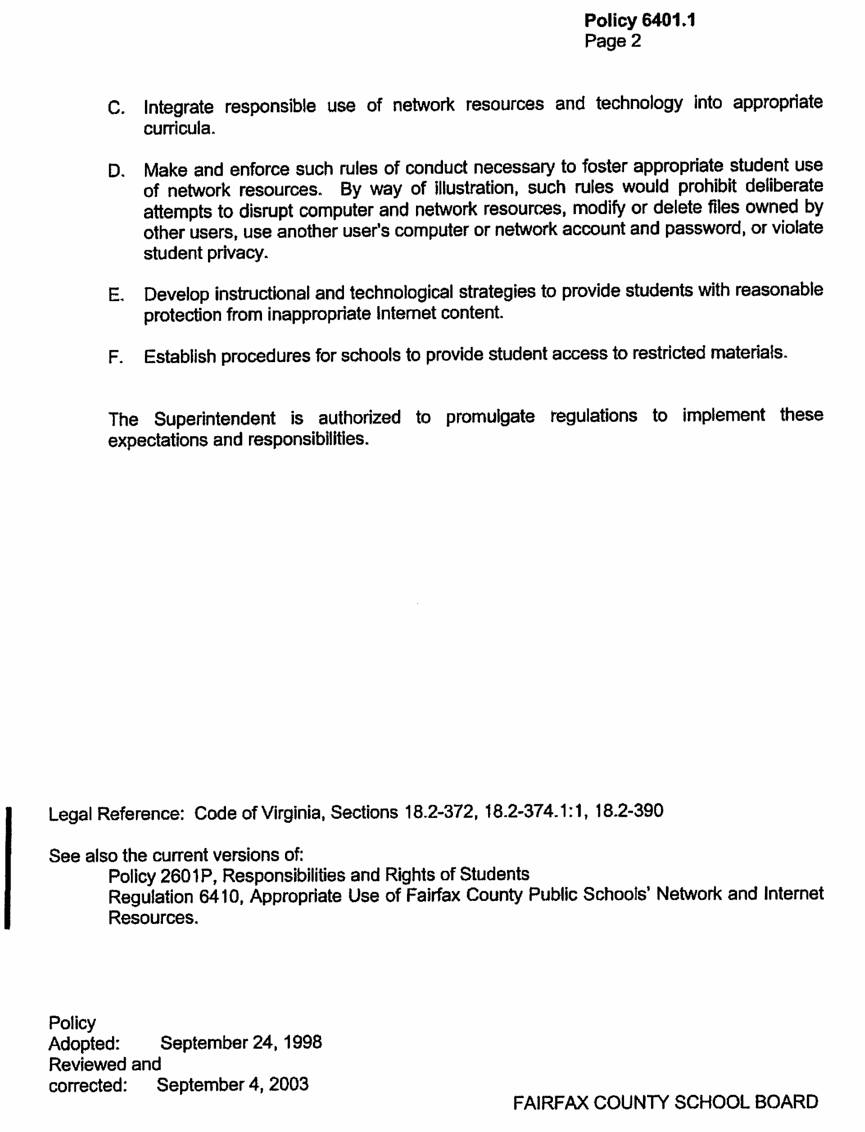
D. Should not arbitrarily restrict student access to content that may support the Program of Studies or other educational purposes.

III. **RESPONSIBILITIES**

In meeting the School Board's expectations, the school division should:

A. Provide information for school staff members and parents to promote a consistent and accurate understanding of the appropriate use of network resources.

B. Educate students and staff members on personal safety practices and effective techniques for identifying and evaluating information and its sources. By way of illustration, personal safety practices include practices that would deter the release of personal student information and meetings with anyone to whom a student corresponded online without the permission of a responsible adult.



Policy 6401.1
Page 2

C. Integrate responsible use of network resources and technology into appropriate curricula.

D. Make and enforce such rules of conduct necessary to foster appropriate student use of network resources. By way of illustration, such rules would prohibit deliberate attempts to disrupt computer and network resources, modify or delete files owned by other users, use another user's computer or network account and password, or violate student privacy.

E. Develop instructional and technological strategies to provide students with reasonable protection from inappropriate Internet content.

F. Establish procedures for schools to provide student access to restricted materials.

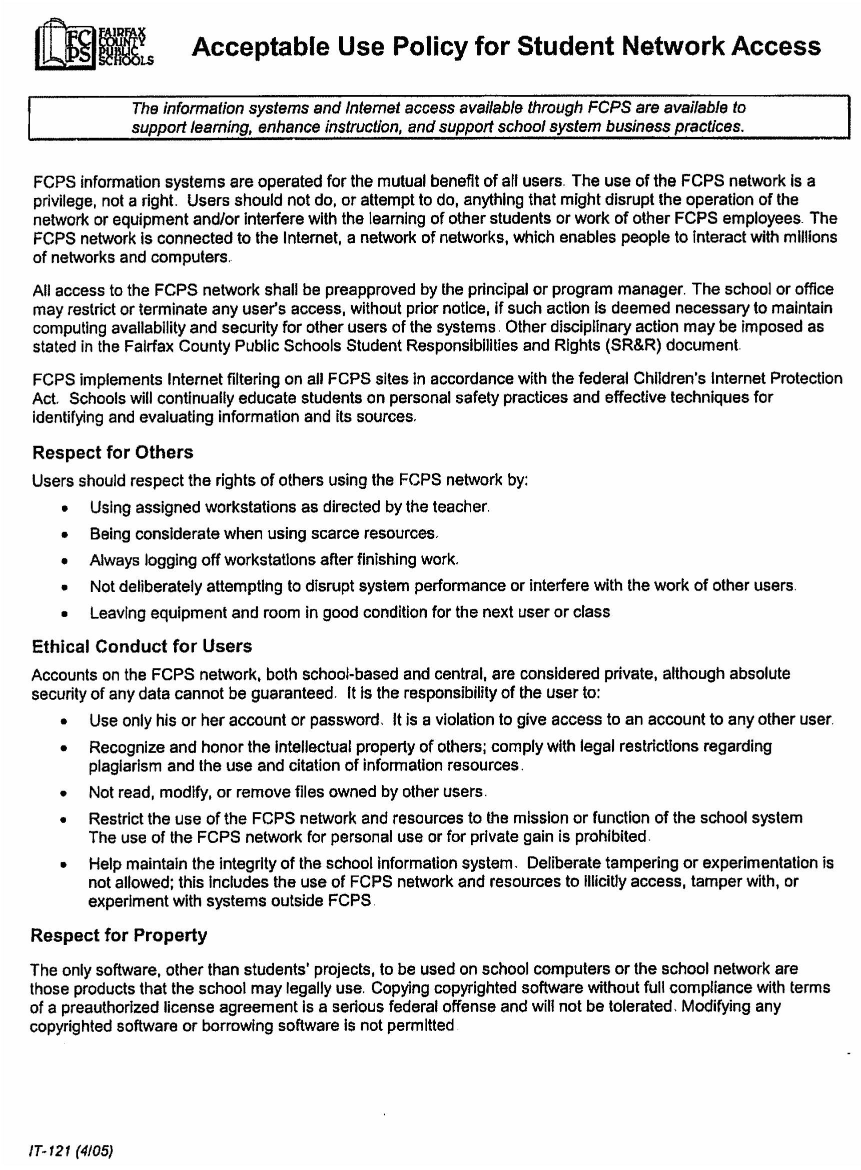
The Superintendent is authorized to promulgate regulations to implement these expectations and responsibilities.

Legal Reference: Code of Virginia, Sections 18.2-372, 18.2-374.1:1, 18.2-390

See also the current versions of:
Policy 2601P, Responsibilities and Rights of Students
Regulation 6410, Appropriate Use of Fairfax County Public Schools' Network and Internet Resources.

Policy
Adopted: September 24, 1998
Reviewed and
corrected: September 4, 2003

FAIRFAX COUNTY SCHOOL BOARD



Acceptable Use Policy for Student Network Access

The information systems and Internet access available through FCPS are available to support learning, enhance instruction, and support school system business practices.

FCPS information systems are operated for the mutual benefit of all users. The use of the FCPS network is a privilege, not a right. Users should not do, or attempt to do, anything that might disrupt the operation of the network or equipment and/or interfere with the learning of other students or work of other FCPS employees. The FCPS network is connected to the Internet, a network of networks, which enables people to interact with millions of networks and computers.

All access to the FCPS network shall be preapproved by the principal or program manager. The school or office may restrict or terminate any user's access, without prior notice, if such action is deemed necessary to maintain computing availability and security for other users of the systems. Other disciplinary action may be imposed as stated in the Fairfax County Public Schools Student Responsibilities and Rights (SR&R) document.

FCPS implements Internet filtering on all FCPS sites in accordance with the federal Children's Internet Protection Act. Schools will continually educate students on personal safety practices and effective techniques for identifying and evaluating information and its sources.

Respect for Others

Users should respect the rights of others using the FCPS network by:

- Using assigned workstations as directed by the teacher.
- Being considerate when using scarce resources.
- Always logging off workstations after finishing work.
- Not deliberately attempting to disrupt system performance or interfere with the work of other users.
- Leaving equipment and room in good condition for the next user or class

Ethical Conduct for Users

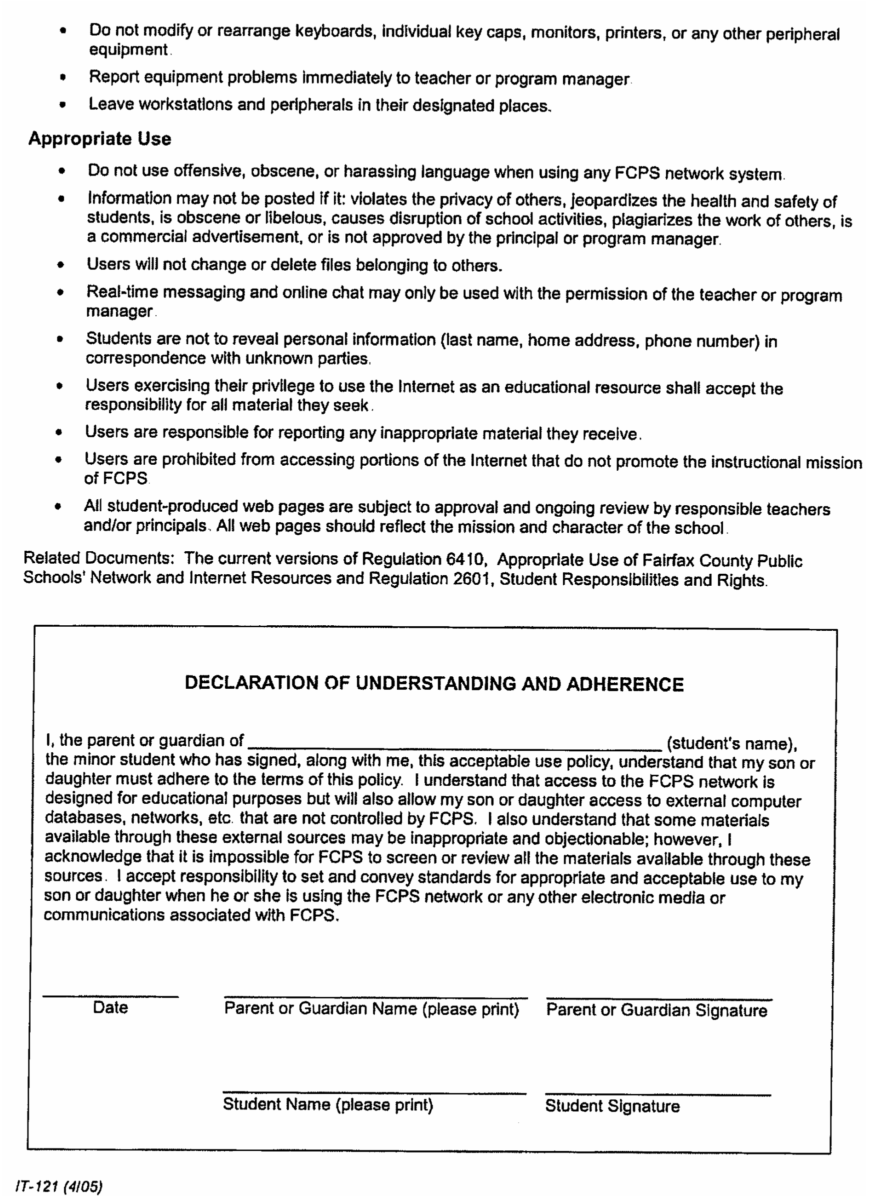
Accounts on the FCPS network, both school-based and central, are considered private, although absolute security of any data cannot be guaranteed. It is the responsibility of the user to:

- Use only his or her account or password. It is a violation to give access to an account to any other user.
- Recognize and honor the intellectual property of others; comply with legal restrictions regarding plagiarism and the use and citation of information resources.
- Not read, modify, or remove files owned by other users.
- Restrict the use of the FCPS network and resources to the mission or function of the school system The use of the FCPS network for personal use or for private gain is prohibited.
- Help maintain the integrity of the school information system. Deliberate tampering or experimentation is not allowed; this includes the use of FCPS network and resources to illicitly access, tamper with, or experiment with systems outside FCPS.

Respect for Property

The only software, other than students' projects, to be used on school computers or the school network are those products that the school may legally use. Copying copyrighted software without full compliance with terms of a preauthorized license agreement is a serious federal offense and will not be tolerated. Modifying any copyrighted software or borrowing software is not permitted

IT-121 (4/05)



- Do not modify or rearrange keyboards, individual key caps, monitors, printers, or any other peripheral equipment.
- Report equipment problems immediately to teacher or program manager.
- Leave workstations and peripherals in their designated places.

Appropriate Use

- Do not use offensive, obscene, or harassing language when using any FCPS network system.
- Information may not be posted if it: violates the privacy of others, jeopardizes the health and safety of students, is obscene or libelous, causes disruption of school activities, plagiarizes the work of others, is a commercial advertisement, or is not approved by the principal or program manager.
- Users will not change or delete files belonging to others.
- Real-time messaging and online chat may only be used with the permission of the teacher or program manager.
- Students are not to reveal personal information (last name, home address, phone number) in correspondence with unknown parties.
- Users exercising their privilege to use the Internet as an educational resource shall accept the responsibility for all material they seek.
- Users are responsible for reporting any inappropriate material they receive.
- Users are prohibited from accessing portions of the Internet that do not promote the instructional mission of FCPS.
- All student-produced web pages are subject to approval and ongoing review by responsible teachers and/or principals. All web pages should reflect the mission and character of the school.

Related Documents: The current versions of Regulation 6410, Appropriate Use of Fairfax County Public Schools' Network and Internet Resources and Regulation 2601, Student Responsibilities and Rights.

DECLARATION OF UNDERSTANDING AND ADHERENCE

I, the parent or guardian of ______________________________ (student's name), the minor student who has signed, along with me, this acceptable use policy, understand that my son or daughter must adhere to the terms of this policy. I understand that access to the FCPS network is designed for educational purposes but will also allow my son or daughter access to external computer databases, networks, etc. that are not controlled by FCPS. I also understand that some materials available through these external sources may be inappropriate and objectionable; however, I acknowledge that it is impossible for FCPS to screen or review all the materials available through these sources. I accept responsibility to set and convey standards for appropriate and acceptable use to my son or daughter when he or she is using the FCPS network or any other electronic media or communications associated with FCPS.

__________ Date

______________________ Parent or Guardian Name (please print)

______________________ Parent or Guardian Signature

______________________ Student Name (please print)

______________________ Student Signature

IT-121 (4/05)

MR. UPTON. Mr. Kelly.

MR. KELLY. Good morning, Chairman Upton, and thank you very much for holding this hearing. I want to personally thank my Representative, Ms. Eshoo, for her warm welcome, and all committee members as well.

My name is Chris Kelley. I serve as Chief Privacy Officer of Facebook, a social utility that allows people to share information easily with their real world communities.

I joined Facebook last September as the first Chief Privacy Officer in the social neatworking space. In my previous role as a chief privacy officer and technology attorney, I represented many clients in the technology media industry on safety privacy issues. I was also part of the founding team and served as a Fellow at Harvard Law School's Berkman Center for Internet and Society, a leading think tank focused on public policy issues of the digital age.

I am happy to be here today to talk about social networking sites generally, and particularly about Facebook. By now you have heard a lot of things about the site. You are also going to hear some positive things, and I understand a number of you have hopefully experienced some of the positives today.

I would like to begin telling you why teenagers and young adults love these sites, and then also about what is special about Facebook and especially our approach to online safety.

Facebook at its core is about community. It is about providing an online way for people to communicate with friends and to meet new ones who are part of their real world communities. It is about providing individuals with avenues for self-expression and creativity. It is about providing the community members with easy ways to learn and share new ideas. For all of these reasons, Facebook is fun and very popular, beginning with college students, and now with high school students and validated work communities.

Although only founded by Mark Zuckerberg, our CEO, in his dorm room in February of 2004, modeled after the paper Facebook that is given to many students at universities, we now have over 800 million users. Facebook is the seventh busiest website in the United States.

Facebook at its inception recognized the community's need to feel safe in order to thrive. As a result, Mark and our other founders placed users' privacy, security, and safety at the center of Facebook's mission and its architecture. It is a radical difference between sites with controlled access based on real world communities and those that make massive amounts of personal information available to anyone on the open Internet.

We implement our safety principles at Facebook with four levels of user protection. First, we require validation. E-mail is the primary token where it is possible for almost all colleges and for about 15 percent of high schools. We use invitations where a school-validated e-mail address is not available.

Second, we place users in individual networks based on the real world school communities and we partition information availability within those networks. This provides a built-in neighborhood watch program where abuse of the system can be easily identified and dressed. So if you are a student at Walt Whitman High School in the Maryland suburbs, you only have access to other students at that high school.

Third, we empower members in our network to make choices about how they reveal information. We offer detailed privacy settings and easy reporting of the violations of our terms of service.

Finally, we have a technology and safety net to detect misuse of the site and protect our members. We employ technology tools that we deploy to detect misuse of the site and human capital dedicated to potential problems. We highlight those accounts. We do an automatic disband when people exceed a certain threshhold, and we examine that member's account to see if they are potentially harming other people on the site.

As a result of these important privacy, security, and safety features, we have very rarely encountered the same unfortunate problems that other social networking sites have been having. Facebook employs these because we recognize there is always a potential for bad actors in any online community, just as in the real world.

We have vigorously sought to support the construction of safe online communities both through our technology tools and other educational developers. More specifically, Facebook supports the educational law enforcement efforts of the Federal Trade Commission. We have been engaged in a dialogue with the National Southern Office of Attorneys General with best practices for social networking sites. WiredSafety.org and I have worked with Parry for quite a number of years, and parents everywhere, because they are ultimately the first line of defense.

We also support the efforts of all companies in the social networking industry to make the world safer and more secure for their members. So, in short, we think the competition to provide social networkers with safer choices is a very good thing, so we commend this committee for its efforts and we welcome the opportunity to serve as a community tie to you.

Facebook is proud to have led the way in giving the people an ability to share and control sharing of information online. With these factors in mind, I would like to offer two quick observations about the Deleting of Online Predators Act.

We are very concerned about the vagueness of the "easily access" or "may easily be subject to" standards that the Deleting of Online Predators Act articulates as a basis for blocking a social networking site. We are not certain there is an effective way for us to articulate the likelihood of such an event, though we do appreciate the attempt to distinguish between a distant possibility and a more easily foreseeable one.

As the committee further considers the legislation, it might examine the possibility of a safe harbor for sites deploying reasonably effective measures to limit general availability of profiles or adult-child interaction through the site. We found that deploying technical tools allowing validation and segmentation of communities effectively limit adult-child interaction.

Second, I would stress that any congressional action should encourage the deployment of technology to protect children and be very conscious of avoiding discouragement of the pro aspects of the online site. There is a reason that children and young adults make these sites major parts of their day: the natural desire of all people to express themselves and share information with friends. It is why a number of you went into politics.

I would encourage you to discuss Facebook with your staffers and interns who are students or recent graduates and let them articulate the sites and the benefits of the sites that it gives to their users. Thank you for the opportunity to comment before the committee, and I look forward to the discussion.

[The prepared statement of Chris Kelly follows:]

PREPARED STATEMENT OF CHRIS KELLY, VICE PRESIDENT, CORPORATE DEVELOPMENT AND CHIEF PRIVACY OFFICER, FACEBOOK

Thank you Chairman Upton, ranking member Markey, and members of the Subcommittee for this opportunity to be with you and explain how Facebook uses technology and policy to protect people on our network.

My name is Chris Kelly, and I serve as Chief Privacy Officer of Facebook, a social utility that allows people to share information with their real world communities. I am very happy to be here today to explain how the two core ideas of social interaction and privacy guide everything that we do, and help protect people on our network. As we say in our basic statement of principles, we believe that people want to share information with their friends and those around them, but they don't necessarily want to share personal information with the entire world.

I joined Facebook last September as the first Chief Privacy Officer in the social networking space, and am creating the role at an Internet company for the fourth time. In my previous service as a Chief Privacy Officer and technology attorney I have represented many clients in the technology and media industries on privacy, security, safety, and intellectual property issues. I was also part of the founding team and served as a Fellow at Harvard Law School's Berkman Center for Internet and Society, a leading think tank focused on public policy issues of the digital age.

In February of 2004, our CEO and Founder Mark Zuckerberg launched the first version of Facebook from his college dorm room. Now, Facebook is the seventh busiest site overall and runs the busiest photo site in the United States, according to independent service ComScore Networks. We have more than 8 million registered members for whom Facebook has become a core part of how they interact within their communities.

Starting with our college communities, we have since expanded to offer school-focused interactions for high-school students, and more recently have followed our graduating students into the work world.

Privacy, security, and safety have been at the forefront of our concerns since the founding of the site. There is one overarching way that Facebook differs from nearly all other social networking sites – profile information is not generally available to the outside world. It is only available to Facebook members inside their individual, validated networks or through confirmed friends. We want to give people extensive power over their ability to share information, and the ability to limit who has access to it.

Of course, no protection mechanism is perfect. But the mere fact that Facebook does not make information available by default to anyone with access to the Internet, combined with the other measures we have taken to focus information sharing on real-world communities, makes a radical difference in the privacy, security, and safety of the Facebook experience.

Following this major differentiator from most sites, we have set up four levels of protection for our members that I would like to outline for you today.

First, we require validation in order to get on the site in the first place. For college students, and those high schools where it is possible, membership in the school community is proven through a valid email associated with that college or school. Where high schools do not offer students email addresses, we have instituted an invitation-based system that is designed to limit even initial access to that school network.

Second, we segment information access within networks based on real-world communities. Being a member of Facebook does not give you access to the profiles of all people on Facebook. You are only allowed to access the profiles of other members at your college, high school, work, or (with explicit user choice) geographic network, and have power to add confirmed friends in other networks. This has two positive effects. First, users are gaining more information about those around them in the real world, which has pro-social effects on campuses around the country. Second, there is a built-in neighborhood watch program, especially with respect to high schools, where abuse of the system can be easily identified and addressed.

Third, we put power in our users' hands to make choices about how they reveal information. I have mentioned already the ability to confirm friends from other networks, and the "My Privacy" tab on every navigation bar throughout the site allows users to make detailed choices about who can see particular pieces of information about them, including their contact information and photos.

Finally, we have a safety net of protection through both technological tools we deploy to detect misuse of the site and human capital dedicated to potential problems -- our 20 person and growing customer service staff, headed by a seasoned veteran and backed up by myself and two other attorneys. Most of our customer service representatives are recent graduates of outstanding colleges, and dedicated Facebook users, so they know the system inside and out. On those rare occasions where someone has attempted to misuse our network, we engage rapidly with the relevant authorities. Because the system is built for accountability with its validation requirements and segmentation of communities, misuse is both deterred and generally detected quickly. We quickly launch an internal investigation and step in where we receive reports of the misuse of Facebook in any way.

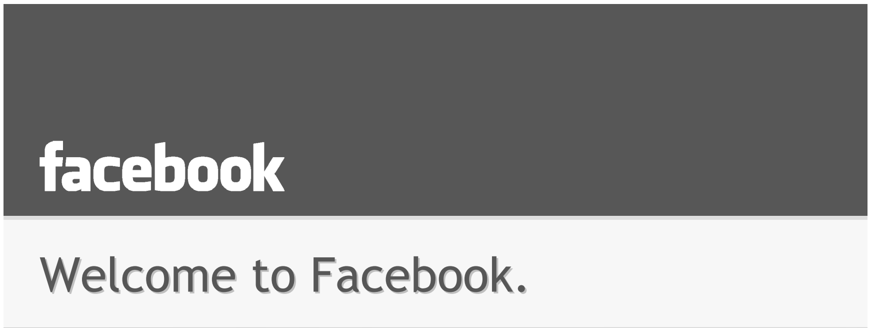
Overall, the fact that information posted on Facebook is not generally available has made Facebook a different experience for our users, and one they clearly enjoy as reflected in their frequent visits. Our intuition about the importance of tying access to information based on the networks where people already exist in real life has been shown to have huge effect in both deterring and exposing misuse. By focusing on real-world networks as the touchstone for access, we provide both a built-in reflection of people's expectations about who will know information about them, and restrictions that make access difficult for those who might have harmful intentions.

Facebook is proud to have led the way in giving people the ability to share, and to control sharing, information online.

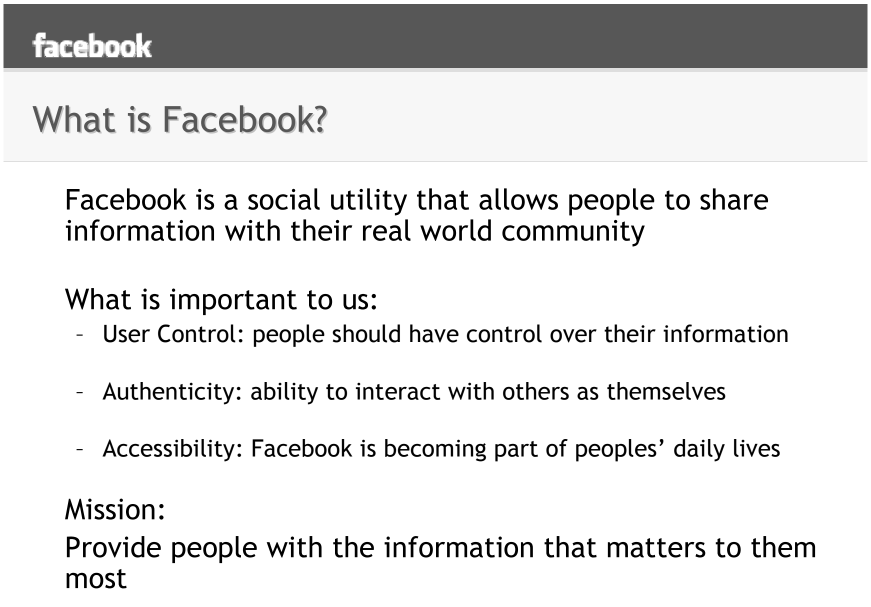
With these factors in mind, I would like to offer two observations. We are very concerned about the vagueness of the “easily access” or “may easily be subject to” standards that the Deleting Online Predators Act articulates as a basis for blocking a social networking site. We are not certain that there is an effective way to articulate likelihood of such an event, though we do appreciate the attempt to distinguish between a distant possibility and a more easily foreseeable one. As the committee further considers the legislation, it might examine the possibility of a “safe harbor” for sites deploying reasonably effective measures to limit general availability of profiles or adult-child interaction through the site. We have found that deploying technological tools allowing validation and segmentation of communities effectively limit adult-child interaction.

Second, I would stress that any Congressional action should encourage the deployment of technology to protect children and be very conscious of avoiding discouragement of the pro-social aspects of online sites. There is a reason that children and young adults make these sites major parts of their day – the natural desire of all people to express themselves and share information with friends. I would encourage you to discuss Facebook with your staffers and interns who are students or recent college graduates and let them articulate the benefits that the site delivers to its more than 8 million users.

Thank you again for the opportunity to comment before the committee, and I look forward to your questions.



Welcome to Facebook.



facebook

What is Facebook?

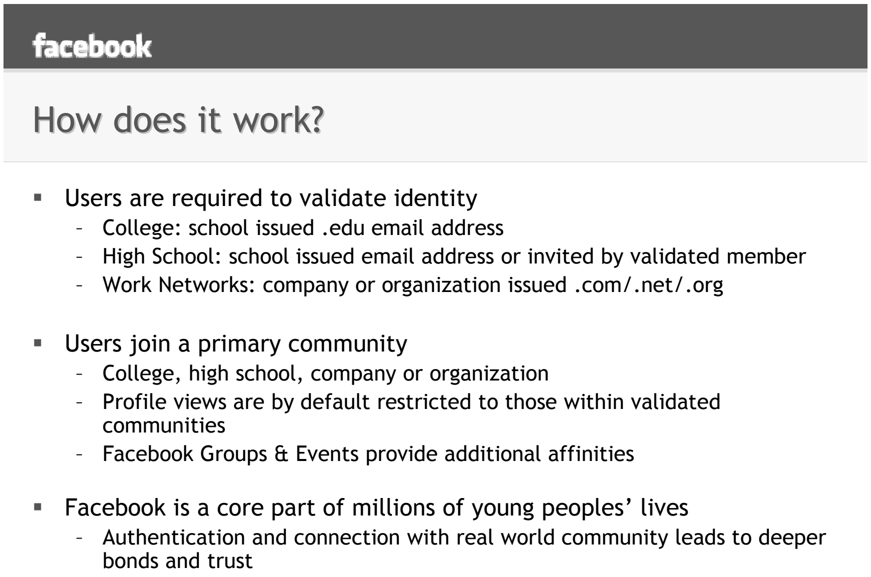
Facebook is a social utility that allows people to share information with their real world community

What is important to us:

- User Control: people should have control over their information
- Authenticity: ability to interact with others as themselves
- Accessibility: Facebook is becoming part of peoples' daily lives

Mission:

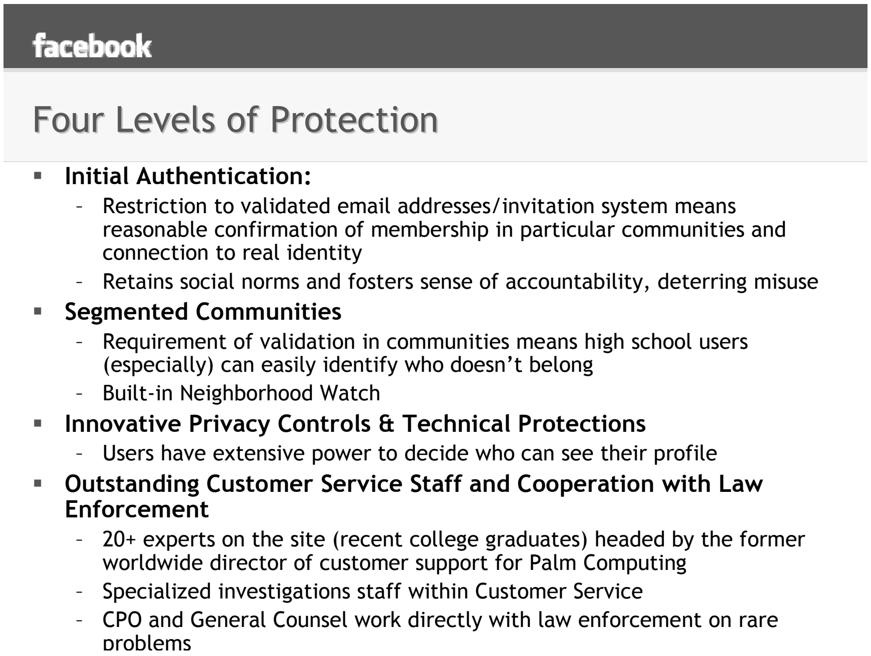
Provide people with the information that matters to them most



facebook

How does it work?

- Users are required to validate identity
  - College: school issued .edu email address
  - High School: school issued email address or invited by validated member
  - Work Networks: company or organization issued .com/.net/.org
- Users join a primary community
  - College, high school, company or organization
  - Profile views are by default restricted to those within validated communities
  - Facebook Groups & Events provide additional affinities
- Facebook is a core part of millions of young peoples' lives
  - Authentication and connection with real world community leads to deeper bonds and trust



facebook

Four Levels of Protection

- **Initial Authentication:**
  - Restriction to validated email addresses/invitation system means reasonable confirmation of membership in particular communities and connection to real identity
  - Retains social norms and fosters sense of accountability, deterring misuse
- **Segmented Communities**
  - Requirement of validation in communities means high school users (especially) can easily identify who doesn't belong
  - Built-in Neighborhood Watch
- **Innovative Privacy Controls & Technical Protections**
  - Users have extensive power to decide who can see their profile
- **Outstanding Customer Service Staff and Cooperation with Law Enforcement**
  - 20+ experts on the site (recent college graduates) headed by the former worldwide director of customer support for Palm Computing
  - Specialized investigations staff within Customer Service
  - CPO and General Counsel work directly with law enforcement on rare problems

MR. UPTON. Ms. Lenhart.

MS. LENHART. Chairman Upton and honorable members of the Subcommittee, it is a privilege for the Pew Internet and American Life Project to be asked to testify at this important hearing.

The project is a nonprofit organization created to examine the social impact of the Internet, with grants from the Pew charitable trust. We at the Pew Internet Project do not take positions on policy questions. Still, we try to do primary research about the impact of people's Internet use that would be helpful to policymakers and other stakeholders.

We have been doing research for 7 years about how teenagers use the Internet and how families are addressing challenges related to new technologies. Our national surveys show that fully 87 percent of Americans between the ages of 12 and 17 go online. Of those that do not currently go online, about half have had some previous Internet experience, which means that in all, 93 percent of American youth have used the Internet at some point.

Their parents use the Internet in large numbers as well; 87 percent of parents with online teens between the ages of 12 and 17 use the Internet compared with 73 percent of all American adults who go online. Our research shows that while parents believe that the Internet can bring both positive opportunity and potential threats into their homes, their overall judgment is that the Internet is a good thing for their children; 67 percent of parents with online teens report this, and their optimism has grown markedly since we first asked the question in year 2000.

This hearing is particularly focused on the role that social networking sites play in teenagers' lives. But it is important to point out the social interaction that takes place online has been an integral, if not an important, part in the Internet experience since the first e-mail was transmitted in 1971.

There are websites where individuals can post information about themselves by creating a profile or website where they can connect with others in the same network. This definition encompasses online dating sites, collaborative software spaces, as well as popular social networking sites like Xanga and Live Journal and places like MySpace, Facebook, and MyYearbook which are based around the creation of a personal profile.

Social networking sites are not the same as chat rooms, though some of these sites do have discussion forums where live chat can take place. The vast majority of communication in online social networks takes place asynchronously and within the network of friends that the user has established.

Other research has recently documented the popularity of social networking sites among teens. A March 2006 survey of 1,160 online teenagers between the ages of 13 and 17 found that 61 percent of teens have personal profiles on sites like MySpace, Friendster, or Xanga, and about half of them have posted photos of themselves somewhere online.

Teenager use of these networks dwarfs that of adults. A Pew Internet Project survey conducted in September of 2005 found that just 16 percent of young adults between the ages of 18 and 29 had used an online social or professional networking site. Older users are even less likely to use the sites.

There are two primary functions of social networking sites that are appealing to teens:

First, the sites enable the user to create sites and share content with others.

Second, the sites enable users to communicate with others using a wide array of messaging, blogging, and posting tools.

Our surveys of teens show that 57 percent of online teens have created some kind of concept for the Internet. This includes blogs, creating websites, posting photos, written material, videos, songs, or other artwork. Much of this content, when posted on social networking sites, is expressive of their view of the world, which can be angry, angst-ridden, or full of idealism. In other words, this is a terrain where teens display their moods in acting out their vision of themselves, sometimes doing it in ways that ignore or downplay risks to their privacy and safety.

Psychologist Erik Erikson argues that most of the work of being an adolescent involves youths' testing as they establish their place in the world. The online environment is for this. It is easy to create materials online and then change it. It enables feedback from peers, the most compelling group of people in teens' lives.

The Internet and social networking sites are the latest iteration in a long line of technologies that have changed the way teenagers communicate and socialize, technologies like the car and the telephone.

The second element of online social networks that contribute to their popularity is that they provide another channel to communicate with others. The act of developing friendships and romantic relationships is also the work of teenagers. And the Internet and its communications applications allow them to do this easily. Our data shows that 89 percent of teens are e-mail users and 75 percent are instant message users. During recent focus groups, we heard from teens that both of these methods of communication were being supplanted in many teens'; lives by the communications tools embedded in social networking websites such as bulletins, messaging, and commenting.

While social networks are attractive for all of the information they enable, there has been considerable information on the dark side. What may seem like harmless disclosure of information, and, in the worst cases, allow them to be tracked and targeted, our most recent work suggests that growing numbers of teens are aware of these problems and are taking steps to address them.

We have just completed a series of focus groups with middle and high schools, that safety and social networking sites has become a major concern of many, if not most, of the teens we interviewed, particularly younger teens and some of the girls. Time and again, these teens detailed their concerns about online predators and the steps they took to keep themselves safe. Sometimes they feel it is sufficient to hit the delete key in response to unwanted messages or requests from strangers. Other times teens in our groups said they would post false information on their sites to protect themselves.

They are now more aware of the dangers of posting information on their profile that might help lurkers find them.

But even as they detailed their fears and concerns about perceived dangers of these sites, they also talked about how important these sites were to them, not just as a place to learn about and share new music, video, or photos, but also as a place that helps them develop and maintain friendships that they rely on for support.

Looking more closely at safety issues, parents and children also agree about some fundamental truths about the online generational divide. Both parents and their children agree that parents are generally less tech-savvy than their children.

Still, 54 percent of parents report having some type of filtering or monitoring software on the home. Two-thirds of parents also take nontechnical steps online by checking on their Web use and placing the computer in a public place in the home. In the end, the picture we get is that teens and their parents are aware of the double-edged nature of technology, and they welcome access to tools and tech needs that help them make informed choices about what they do online.

I thank you for the opportunity to speak to the committee and I look forward to answering any questions you may have.

[The prepared statement of Amanda Lenhart follows:]

PREPARED STATEMENT OF AMANDA LENHART, SENIOR RESEARCH SPECIALIST, PEW INTERNET AND AMERICAN LIFE PROJECT

Chairman Upton and honorable members of the Subcommittee, it is a privilege for the Pew Internet & American Life Project to be asked to testify at this important hearing. The Project is a nonprofit, nonpartisan research center created to examine the social impact of the internet with grants from the Pew Charitable Trusts. We at the Pew Internet Project do not take positions on policy questions or endorse industry sectors, organizations, or individuals. Still, we try to do primary research about the impact of people's internet use that would be helpful to policy makers and other stakeholders as they consider ideas to improve technology or mitigate its harms.

There is pervasive use of the internet among teenagers

We have been doing research for seven years about how teenagers use the internet and how families are addressing challenges related to new technologies. Our national surveys show that internet use is pervasive among teens and that families are spending time trying to work through all the issues that brings into their homes.

Fully 87% of Americans of middle- and high-school age – those between the ages of 12 and 17 – go online. Of those that do not currently go online, about half have had some previous internet experience, which means that, in all, 93% of American youth have used the internet at some point.

Their parents use the internet in large numbers as well – 87% of parents with teens between the ages of 12 and 17 use the internet, compared with 73% of all American adults who go online. It is clear that many parents extend themselves financially to buy computers and internet access in the belief that mastery of high-tech skills is a prerequisite for their children's future success.

Weighing the pluses and minuses, parents think the internet is a benefit to their children

Indeed, while parents believe that the internet can bring both positive opportunities and potential threats into their homes, their overall judgment is that the internet is a good thing for their children: 67% of parents with online teens report this, and their optimism has grown markedly since we first asked the question in the year 2000.

This hearing is particularly focused on the role social networking websites such as MySpace.com and Facebook.com play in teenagers' lives. But it is important to point out that social interaction takes place in a wide variety of contexts online and has been an integral part – if not *the most compelling part* – of internet experience since the first email was transmitted in 1971.

Online social networks are popular among teenagers

Our working definition of online social networks is broad. They are "web spaces where individuals can post information about themselves, usually by creating a profile or website, and where they can connect with others in the same network." This definition encompasses online dating sites, some instant messaging tools, collaborative software spaces, as well as popular social networking web sites like Xanga and Live Journal, which are built mainly around connecting friends via their blogs, and places like MySpace, Facebook, Tagged.com, and MyYearbook.

Social networking sites are not the same as chatrooms, though some of these sites do have discussion forums where live chat can take place. The vast majority of communication in online social networks takes place asynchronously and within the network of "friends" that the user has established.

Other research has recently documented the popularity of social networking sites among teens. A March 2006 survey of 1,160 online teenagers between the ages of 13 and 17 found that 61% of teens have personal profiles on sites like MySpace, Friendster or Xanga, and about half of them have posted pictures of themselves somewhere online.[1]

Teenagers' use of these networks appears to dwarf that of adults. A Pew Internet Project survey conducted in September 2005 found that just 16% of young adult internet users between the ages of 18-29 had used an online social or professional networking site. Older users are even less likely to use the sites.

Social network sites are popular because they enable new expression and activities that appeal to teenagers

There are two primary functions of social networking sites that are especially appealing to teens:

- First, the sites enable users to create and share content with others -- generally, this is content that is expressive of users' identities.
- Second, the sites enable users to communicate with others using a wide array of messaging, blogging and posting tools.

New online tools help teens explore their identities

Our surveys of teens show that 57% of online teens have created some kind of content for the internet. This includes blogging, creating websites, posting photos, written material, videos, songs, or other artwork. Teens also remix content they find online into something new and share that online with others. Much of this content when posted on social networking or other websites is expressive of their view of the world – a view that can be playful, angry, riveting, revolting, angst-ridden, hilarious, or full of idealism. In other words, this is a terrain where teens display their moods and act out their vision of themselves – sometimes doing it in ways that ignore or downplay risks to their privacy and safety

Psychologist Erik Erikson argues that much of the "work" of being an adolescent involves youths' testing of their identities as they establish their place in the world. The online environment offers many opportunities to do this type of developmental "work." It's easy to create material and change it when the mood strikes. Most importantly, it enables feedback from peers – the group about which teens are most keenly interested.

[1] See the press release from Cox Communications and link to full results here: http://www.cox.com/takecharge/survey_results.asp

The internet and social networking sites are the latest iteration in a long line of technologies that have changed the way teenagers communicate and socialize. As historian Beth L. Bailey notes in her book, *From Front Porch to Back Seat*, the invention of the automobile, which brought youth radically new levels of mobility and privacy in the early 20th Century, is often credited as the technological catalyst that spurred a new and controversial social practice among young men and women called "dating."[2]

Staying in touch with peers is a big draw

The second element of online social networks that contributes to their popularity is that they provide another channel for teens to communicate with others, especially with those who are connected through a visible web. The act of developing friendships and romantic relationships is also the "work" of teenagers, and the internet and its communications applications allow them to do this.

Our data show that 89% of teens are email users and 75% are instant message users. During recent focus groups, we heard from teens that both of these methods of communication were being supplanted in many teens' lives by the communications tools embedded in social networking websites -- such as "bulletins," messaging, and commenting.

Teens, especially younger youth and girls, are developing new awareness about the risks of some disclosures on social network sites

While social network sites are attractive for all the content and communication they enable, there has been considerable public attention focused on the dark side of all this public disclosure by teenagers. What may seem like harmless disclosures of information can sometimes compromise teens' privacy and, in the worst cases, allow them to be tracked and targeted.

Our most recent work suggests that growing numbers of teens are aware of these problems and are taking steps to address them. We have just completed a series of focus groups with middle and high school students and it was striking to note that safety on social networking sites has become a major concern of many if not most teens we interviewed, particularly younger teens and girls.

Time and again, these teens detailed their concerns about online predators and the steps they took to keep themselves safe. Sometimes they feel it is sufficient to hit the delete key in response to unwanted messages or requests from strangers. Other times, the teens in our groups said they would post false ages on their sites. Often, they would say they were younger than they actually were because privacy protections at some social network sites are stronger for younger users. Finally, these teens told us that they are more aware now of the dangers of posting information in their profiles that might help lurkers find them.

Even as they detailed their fears and concerns about the perceived dangers of these sites, they also talked about how important these sites were to them – not just as place to learn about and share new music, video, or photos, but also as a place that helps them develop and maintain friendships that they rely on for support.

Parents and children agree there is a generational divide in many households

Looking more closely at safety issues, parents and children also agree about some of the fundamental truths that characterize the online generational divide. Both parents and

[2] Bailey discusses the shift from the old practice of "calling" whereby a male suitor would arrive at the house of a young woman "expecting to be received in her family's parlor, to talk, to meet her mother, perhaps to have some refreshments or to listen to her play the piano" to the new practice of "dating" whereby the young woman would expect to be "taken 'out' somewhere and entertained." See p. 13 for this reference and p.19 for a discussion of the automobile's influence in this transition.

their children agree that parents are generally less tech savvy than their children. In addition:

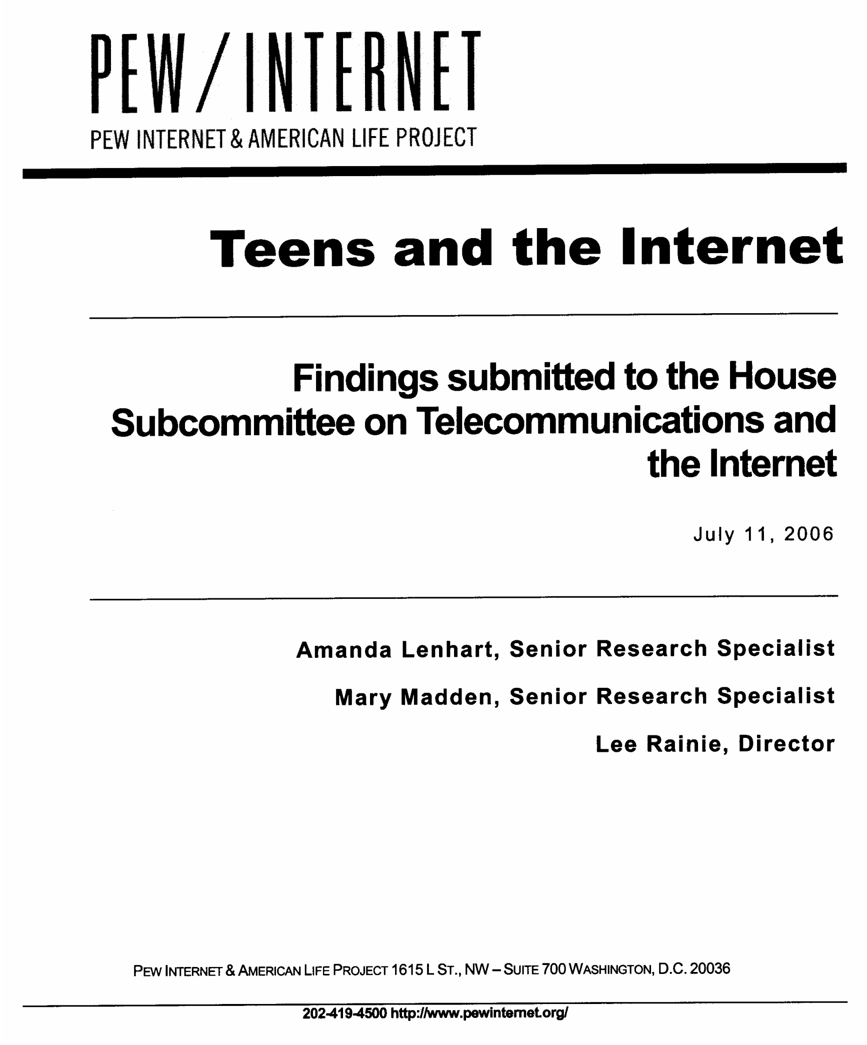
- 81% of parents and 79% of teens agree that children are not as careful as they should be about the information they give out online
- 62% of parents with online teens and 62% of online teens agree that children do things online that they wouldn't want their parents to know about.

Many parents try to take steps to safeguard their children

Still, 54% of parents report having some type of filtering or monitoring software installed on a computer in the home. Two thirds of parents also take non-technical steps to protect their children online, by checking up on their web use, setting rules and time limits and placing the computer in a public place in the home.

In the end, the picture we get is that teens and their parents are aware of the double-edged nature of technology, and they welcome access to tools and techniques that help them make informed choices about what they do online.

Thanks again for the opportunity to speak to the committee today and I look forward to answering any questions you may have.



PEW/INTERNET

PEW INTERNET & AMERICAN LIFE PROJECT

Teens and the Internet

Findings submitted to the House Subcommittee on Telecommunications and the Internet

July 11, 2006

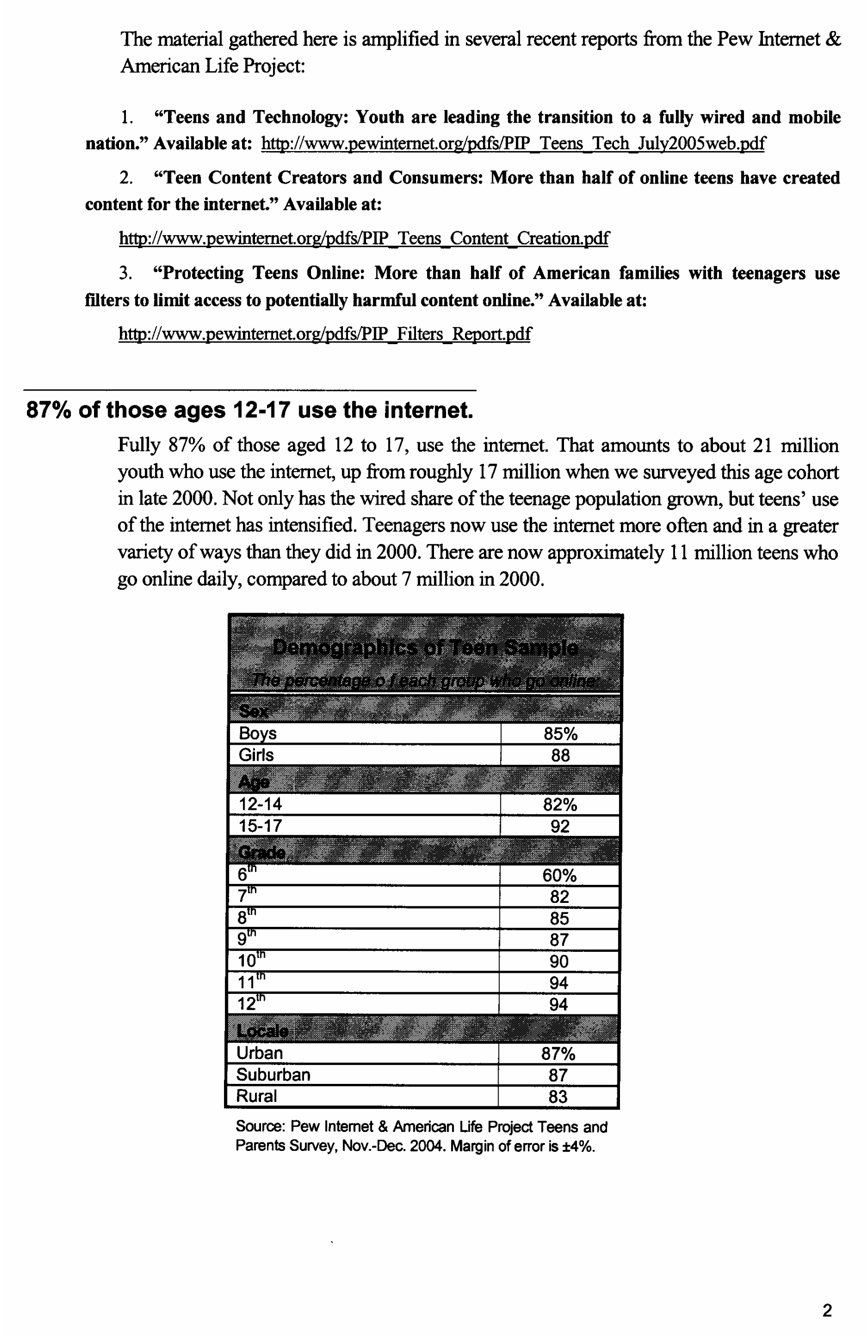
Amanda Lenhart, Senior Research Specialist

Mary Madden, Senior Research Specialist

Lee Rainie, Director

PEW INTERNET & AMERICAN LIFE PROJECT 1615 L ST., NW – SUITE 700 WASHINGTON, D.C. 20036

202-419-4500 http://www.pewinternet.org/



The material gathered here is amplified in several recent reports from the Pew Internet & American Life Project:

1. **"Teens and Technology: Youth are leading the transition to a fully wired and mobile nation." Available at:** http://www.pewinternet.org/pdfs/PIP_Teens_Tech_July2005web.pdf

2. **"Teen Content Creators and Consumers: More than half of online teens have created content for the internet." Available at:**

http://www.pewinternet.org/pdfs/PIP_Teens_Content_Creation.pdf

3. **"Protecting Teens Online: More than half of American families with teenagers use filters to limit access to potentially harmful content online." Available at:**

http://www.pewinternet.org/pdfs/PIP_Filters_Report.pdf

87% of those ages 12-17 use the internet.

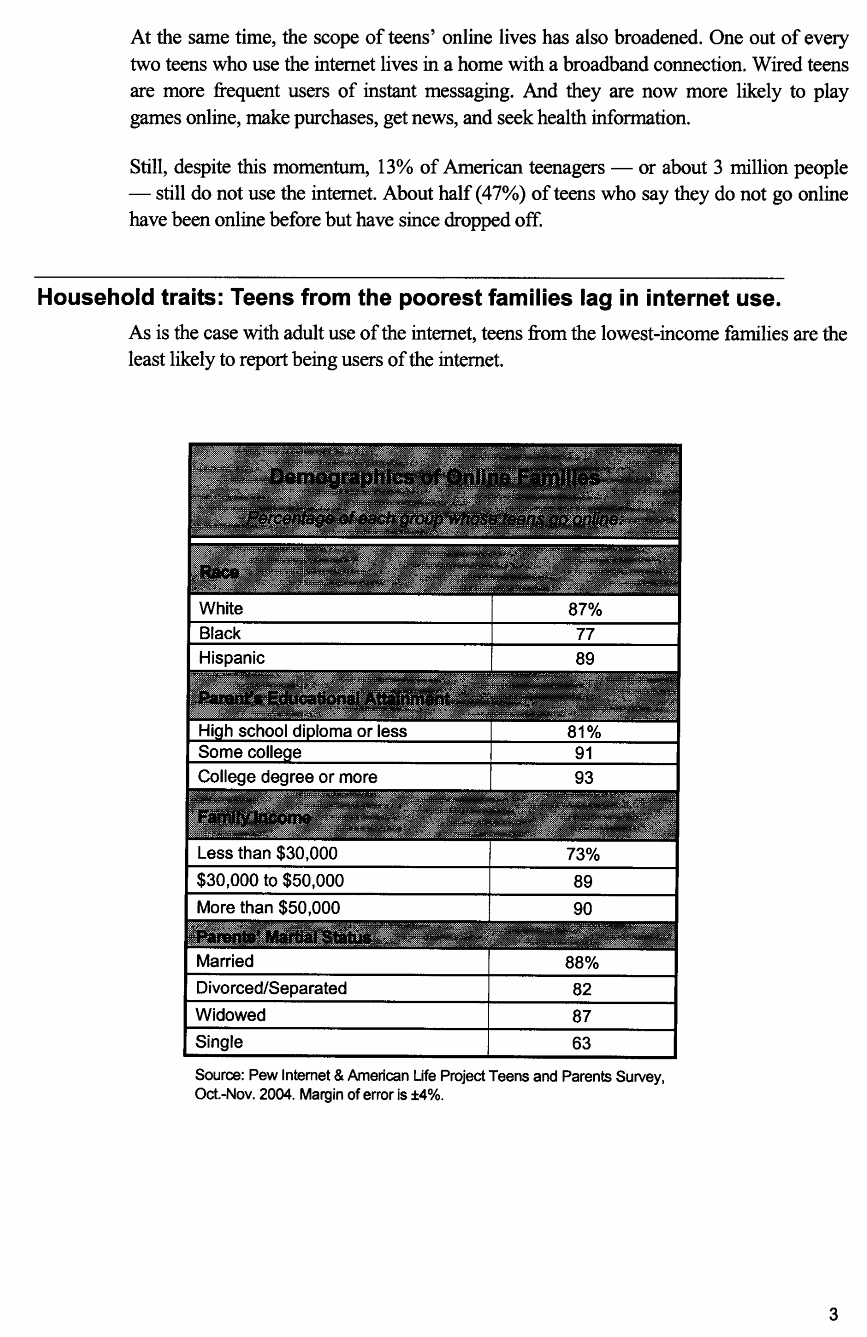
Fully 87% of those aged 12 to 17, use the internet. That amounts to about 21 million youth who use the internet, up from roughly 17 million when we surveyed this age cohort in late 2000. Not only has the wired share of the teenage population grown, but teens' use of the internet has intensified. Teenagers now use the internet more often and in a greater variety of ways than they did in 2000. There are now approximately 11 million teens who go online daily, compared to about 7 million in 2000.

Demographics of Teen Sample

The percentage of each group who go online

Sex	
Boys	85%
Girls	88
Age	
12-14	82%
15-17	92
Grade	
6th	60%
7th	82
8th	85
9th	87
10th	90
11th	94
12th	94
Locale	
Urban	87%
Suburban	87
Rural	83

Source: Pew Internet & American Life Project Teens and Parents Survey, Nov.-Dec. 2004. Margin of error is ±4%.



At the same time, the scope of teens' online lives has also broadened. One out of every two teens who use the internet lives in a home with a broadband connection. Wired teens are more frequent users of instant messaging. And they are now more likely to play games online, make purchases, get news, and seek health information.

Still, despite this momentum, 13% of American teenagers — or about 3 million people — still do not use the internet. About half (47%) of teens who say they do not go online have been online before but have since dropped off.

Household traits: Teens from the poorest families lag in internet use.

As is the case with adult use of the internet, teens from the lowest-income families are the least likely to report being users of the internet.

Demographics of Online Families *Percentage of each group whose teens go online:*	
Race	
White	87%
Black	77
Hispanic	89
Parent's Educational Attainment	
High school diploma or less	81%
Some college	91
College degree or more	93
Family Income	
Less than $30,000	73%
$30,000 to $50,000	89
More than $50,000	90
Parents' Martial Status	
Married	88%
Divorced/Separated	82
Widowed	87
Single	63

Source: Pew Internet & American Life Project Teens and Parents Survey, Oct.-Nov. 2004. Margin of error is ±4%.

Teens are technology rich and enveloped by a wired world.

An overwhelming majority of all teenagers, 84%, report owning at least one personal media device: a desktop or laptop computer, a cell phone or a Personal Digital Assistant (PDA). 44% say they have two or more devices, while 12% have three and 2% report having all four of those types of devices. Only 16% of all teens report that they do not have any of these devices at all.

Parental use of filters to protect youth online is growing.

Some 54% of parents of online teens report having a filter installed on their home computer, up from 41% of parents of online teens in the Pew Internet & American Life Project survey in December 2000.

In addition to employing filters, parents are trying other methods to stay abreast of their children's online activities.

Many families are heeding the message from safety advocates about placing the family's internet-connected computer or computers in public places within the home. And most parents say they have established rules about their children's computer use.

- 73% of online teens say their household computer is located in a public place inside the house.
- 64% of parents of online teenagers say they set rules about their children's time online.

However, there are still large gaps in perception about how much parent-child monitoring is taking place: Most teens do *not* believe their parents are checking up on them, while most parents say they are.

- 62% of parents report checking up on their child's surfing habits after he or she has gone online …
- …but only 33% of teens who use the internet from home say they believe their parents monitor their online activity.

The impact of filters and parental vigilance remains unclear: Parents *and* teens agree that teens are not careful enough online, and both believe that teens do things online that their parents would not approve of.

There is striking consensus among parents and their teens that the teenage population is not as careful as it should be online and that teens do things online their parents don't know about.

- 81% of parents of online teens say that teens aren't careful enough when giving out information about themselves online; 79% of online teens agree.

- ■ 65% of all parents and 64% of all teens say that teens do things online that they wouldn't want their parents to know about.

Bad experiences online keep some teens away from the internet.

Some 13% of youth between the ages of 12 and 17 – about 3 million teens – do not use the internet. Nearly half (47%) of these non-users say they used the internet at one point or another, but then dropped off. About one in ten of all non-online teens report being offline because they had bad experiences, they face parental restrictions, or because they do not feel safe. At the same time, non-internet using teens were more likely to say that lack of interest, lack of time, or lack of access were the major reasons they were not online.

Teens log on most often from home, but library use grows more than any other location.

The vast majority of online teens report going online from home and say that it is the place they go online most often. Close to nine in ten (87%) of teen internet users say they go online from home.

Seventy-eight percent of online teens report that they go online from school, up from 64% of online teens in 2000. Accessing the internet from a friend or relative's house is also on the rise, with 74% of teens reporting that they access the internet from those locations, up from 64% in 2000.

More than half (54%) of all online teens say they have gone online from a library, up from a little more than a third of teens (36%) who reported utilizing library internet resources in 2000. Nine percent of teens say they access the internet from a community center, like a Boys' or Girls' club, or a religiously affiliated youth center.

Where teens log on

The places where wired teens have ever gone online and where they go online most often:

	Ever	Most often
Home	87%	74
School	78	17
A Friend's House	74	N/A
Library	54	N/A
Community Center, Youth Center, House of Worship	9	N/A

Source: Pew Internet & American Life Project Teens and Parents Survey, Nov.-Dec. 2004. Margin of error is ±4%.

Email is still a fixture in teens' lives, but instant messaging is preferred.

In all, 89% of online teens report ever using email. Reponses to other questions in our survey and our qualitative research with middle-school- and high-school-aged teens suggest that the popularity of email and the intensity of its use are waning in favor of instant messaging.

Teens' IM use eclipses that of adults.

Teens' love affair with instant messaging has continued full-throttle since 2000. Overall, three-quarters of online teens (75%) — and 65% of all teens — say they use instant messaging. The overall number of teen IM users has grown as the population of online teens has grown. As of our current survey, about 16 million teens have used instant messaging now, up from close to 13 million in 2000.

Adults continue to lag far behind teens in adoption of instant messaging. Overall, only 42% of online adults reported using instant messaging in a recent survey of adults.[1]

IM offers ways for teens to express their identity and reshape technology to their purposes.

Some IM programs offer the option to post a profile that is visible to other IM users and may be made public to the world at large. More than half (56%) of all instant messaging users — or 36% of all teens — report they have created an IM profile and have posted it so that others can see it. In comparison, our survey of adults (18 and older) in early 2004 showed that just one-third (34%) of IM users had posted a profile.

Eighty-six percent of instant messaging teens — or about 56% of all teens — have ever posted an away message, compared to 45% of IM-using adults. Among teen IM users, almost two in five (39%) post an away message every day or almost every day. Among adults, that number drops to 18%.

Most teens will block messages from those they want to shun or avoid.

Communication via instant messaging is not always a positive exchange of pleasantries and conversation. Many instant-message-using teens report blocking someone from communicating with them through IM. In all, 82% of the roughly 16 million IM using teens have ever blocked someone, compared to 47% of IM-using adults who report engaging in this behavior.

Away messages can also be used to dodge conversation partners. Focus group teens describe setting up an away message that remains up even when the user has returned to the screen. One young woman told us:

[1] From the Pew Internet Project's May-June 2004 survey. (n=1,399)

> "I have a version where I can have my away message up, but I can still talk to people and my away message won't go down. So if I don't want to talk to somebody, then I just put up [that] away message and talk to the people that I want to and the other people I can avoid."

More than half of online teens are Content Creators.

Some 57% of online teens create content for the internet. That amounts to half of all teens ages 12-17, or about 12 million youth. These Content Creators report having done one or more of the following activities: create a blog; create or work on a personal webpage; create or work on a webpage for school, a friend, or an organization; share original content such as artwork, photos, stories, or videos online; or remix content found online into a new creation.

- 33% of online teens share their own creations online, such as artwork, photos, stories, or videos.
- 32% say that they have created or worked on webpages or blogs for others, including those for groups they belong to, friends or school assignments.
- 22% report keeping their own personal webpage.
- 19% have created their own online journal or blog.
- About one in five internet-using teens (19%) says they remix content they find online into their own artistic creations.

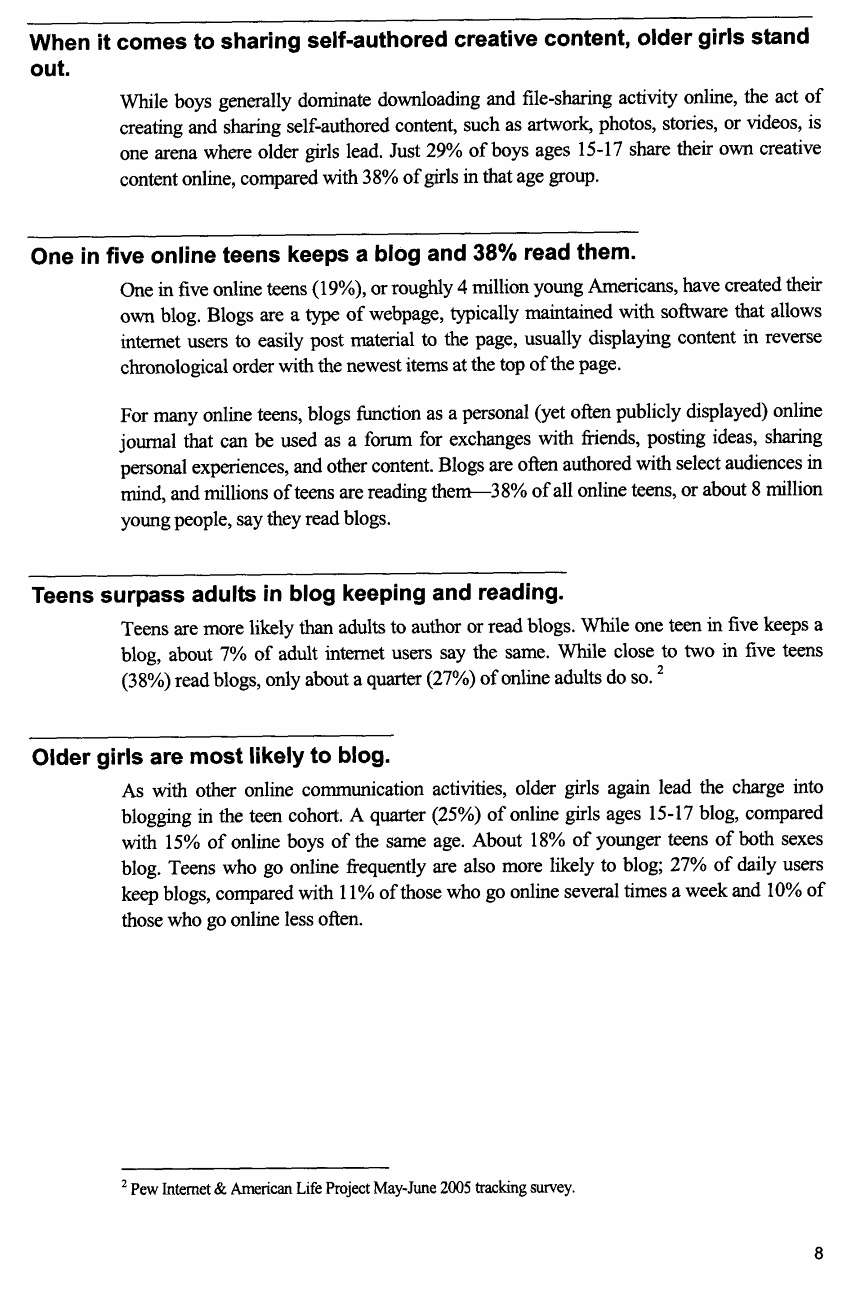
Demographics of Online Teens Who Share Self-Created Media

The percentage of internet users in each group who share content they have created:

[Note: statistically significant differences are highlighted in bold]

Sex	
Boys	31%
Girls	35
Age	
12-14	32%
15-17	34
Family Income	
Less than $30,000 annually	36%
$30,000 - $49,999	35
$50,000 - $74,999	33
$75,000 +	30
Locale	
Urban	**40%**
Suburban	**28**
Rural	34

Source: Pew Internet & American Life Project Teens and Parents Survey, Nov.-Dec. 2004. Margin of error is ±6% for original content sharers.



When it comes to sharing self-authored creative content, older girls stand out.

While boys generally dominate downloading and file-sharing activity online, the act of creating and sharing self-authored content, such as artwork, photos, stories, or videos, is one arena where older girls lead. Just 29% of boys ages 15-17 share their own creative content online, compared with 38% of girls in that age group.

One in five online teens keeps a blog and 38% read them.

One in five online teens (19%), or roughly 4 million young Americans, have created their own blog. Blogs are a type of webpage, typically maintained with software that allows internet users to easily post material to the page, usually displaying content in reverse chronological order with the newest items at the top of the page.

For many online teens, blogs function as a personal (yet often publicly displayed) online journal that can be used as a forum for exchanges with friends, posting ideas, sharing personal experiences, and other content. Blogs are often authored with select audiences in mind, and millions of teens are reading them—38% of all online teens, or about 8 million young people, say they read blogs.

Teens surpass adults in blog keeping and reading.

Teens are more likely than adults to author or read blogs. While one teen in five keeps a blog, about 7% of adult internet users say the same. While close to two in five teens (38%) read blogs, only about a quarter (27%) of online adults do so. [2]

Older girls are most likely to blog.

As with other online communication activities, older girls again lead the charge into blogging in the teen cohort. A quarter (25%) of online girls ages 15-17 blog, compared with 15% of online boys of the same age. About 18% of younger teens of both sexes blog. Teens who go online frequently are also more likely to blog; 27% of daily users keep blogs, compared with 11% of those who go online several times a week and 10% of those who go online less often.

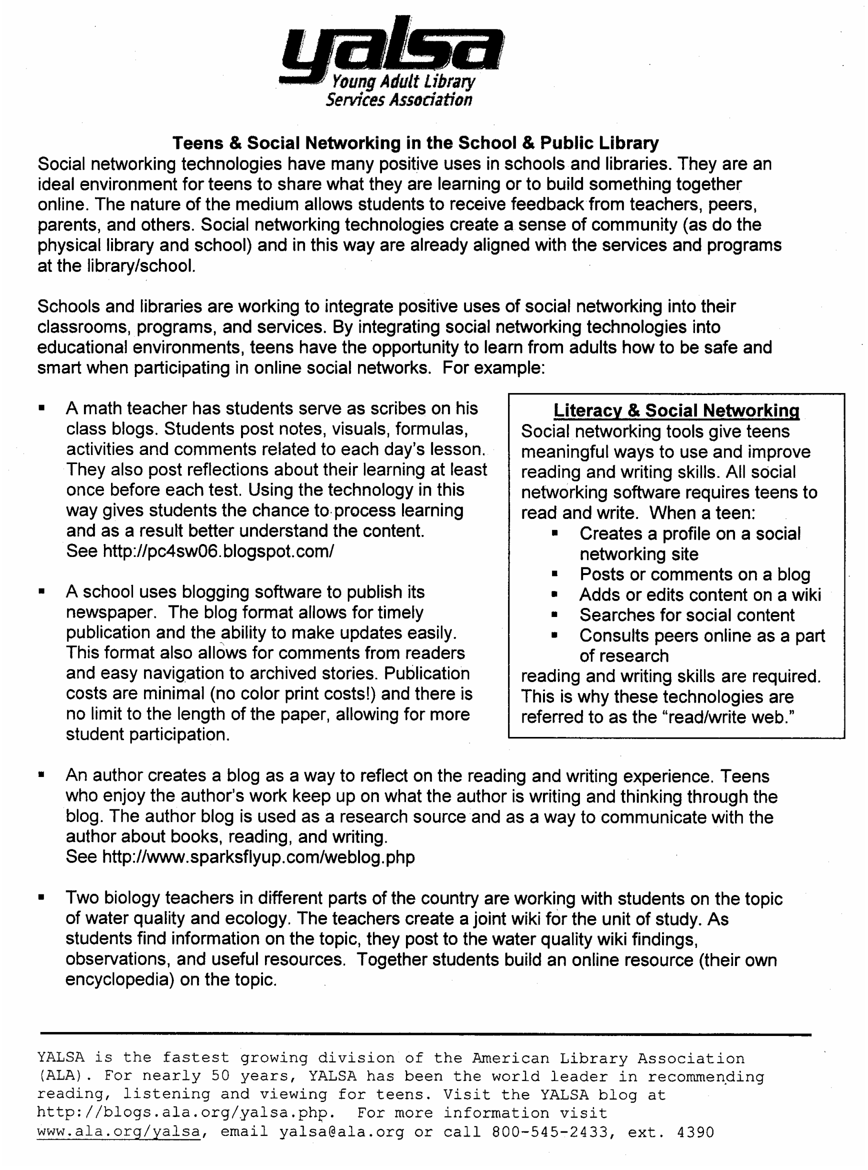
[2] Pew Internet & American Life Project May-June 2005 tracking survey.

MR. UPTON. Ms. Yoke.

MS. YOKE. I would like to ask your permission to insert this document into the record.

MR. UPTON. Without objection.

[The Information follows:]



yalsa
Young Adult Library
Services Association

Teens & Social Networking in the School & Public Library

Social networking technologies have many positive uses in schools and libraries. They are an ideal environment for teens to share what they are learning or to build something together online. The nature of the medium allows students to receive feedback from teachers, peers, parents, and others. Social networking technologies create a sense of community (as do the physical library and school) and in this way are already aligned with the services and programs at the library/school.

Schools and libraries are working to integrate positive uses of social networking into their classrooms, programs, and services. By integrating social networking technologies into educational environments, teens have the opportunity to learn from adults how to be safe and smart when participating in online social networks. For example:

- A math teacher has students serve as scribes on his class blogs. Students post notes, visuals, formulas, activities and comments related to each day's lesson. They also post reflections about their learning at least once before each test. Using the technology in this way gives students the chance to process learning and as a result better understand the content. See http://pc4sw06.blogspot.com/

- A school uses blogging software to publish its newspaper. The blog format allows for timely publication and the ability to make updates easily. This format also allows for comments from readers and easy navigation to archived stories. Publication costs are minimal (no color print costs!) and there is no limit to the length of the paper, allowing for more student participation.

- An author creates a blog as a way to reflect on the reading and writing experience. Teens who enjoy the author's work keep up on what the author is writing and thinking through the blog. The author blog is used as a research source and as a way to communicate with the author about books, reading, and writing. See http://www.sparksflyup.com/weblog.php

- Two biology teachers in different parts of the country are working with students on the topic of water quality and ecology. The teachers create a joint wiki for the unit of study. As students find information on the topic, they post to the water quality wiki findings, observations, and useful resources. Together students build an online resource (their own encyclopedia) on the topic.

Literacy & Social Networking

Social networking tools give teens meaningful ways to use and improve reading and writing skills. All social networking software requires teens to read and write. When a teen:

- Creates a profile on a social networking site
- Posts or comments on a blog
- Adds or edits content on a wiki
- Searches for social content
- Consults peers online as a part of research

reading and writing skills are required. This is why these technologies are referred to as the "read/write web."

YALSA is the fastest growing division of the American Library Association (ALA). For nearly 50 years, YALSA has been the world leader in recommending reading, listening and viewing for teens. Visit the YALSA blog at http://blogs.ala.org/yalsa.php. For more information visit www.ala.org/yalsa, email yalsa@ala.org or call 800-545-2433, ext. 4390

- A public library creates a My Space site as a way to connect with teens in the community. The space includes quick and easy access to the library catalog and other research tools. It includes information on programs and services at the library in which teens can take part. Teens who are not traditional library users learn about and use the library through My Space because they are familiar and comfortable with the technology. Teens make the library one of their My Space friends and are reminded of the library when they log onto their space.
  See ImaginOn Library Loft, http://www.myspace.com/libraryloft
  Hennepin County Library, http://www.myspace.com/hennepincountylibrary

Developmental Assets & Social Networking

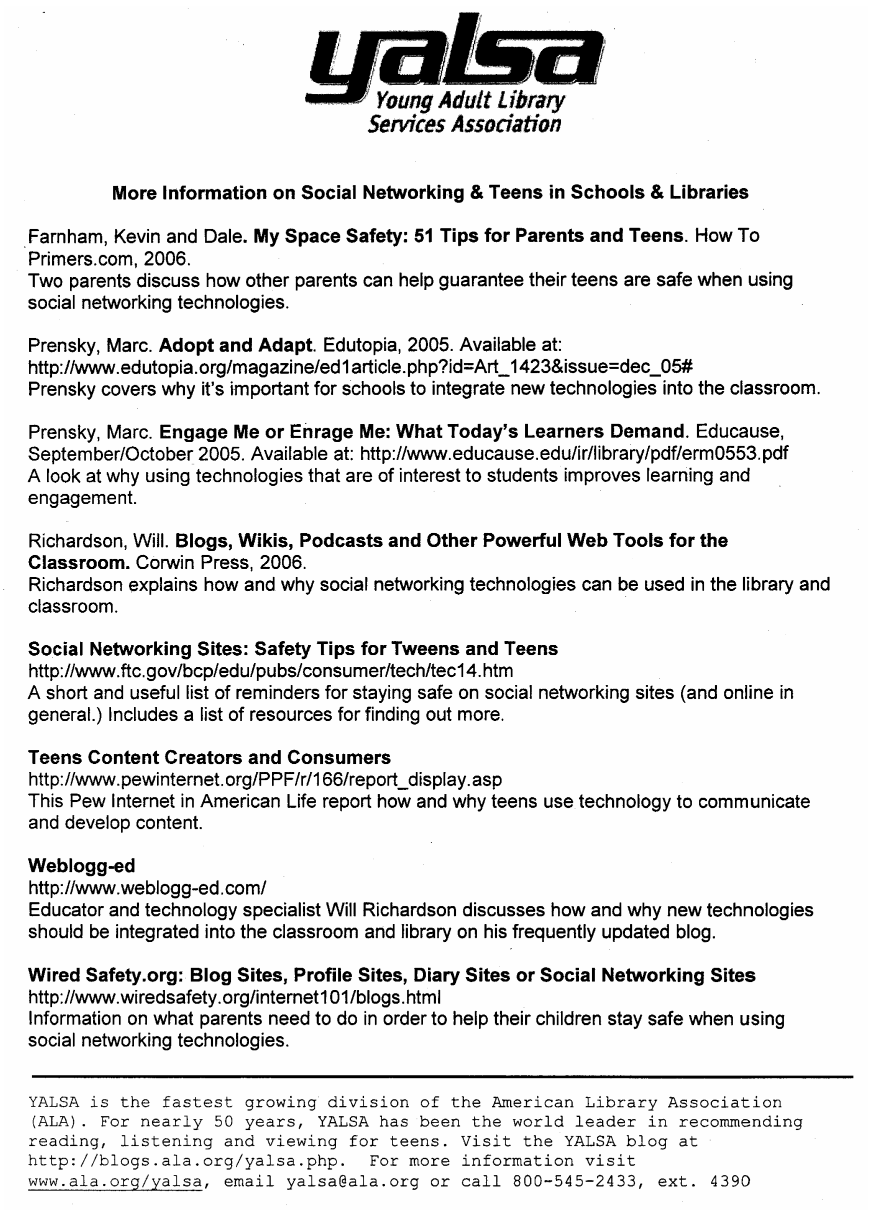
When schools and libraries help teens use social networking tools safely and smartly, they also help teens meet their developmental assets as defined by the Search Institute. (http://www.search-institute.org) For example when teens:

- Learn how to use blogs, wikis, and My Space sites within an educational context they learn about **boundaries and expectations**.
- Are able to use social networking tools in learning they develop a **commitment to learning.**
- Have the opportunity to communicate with peers, experts, authors, etc. via online social networking they develop **social & cultural competence**.
- Work with adults and peers on developing social network sites and teaching others how to use these sites they are **empowered.**
- Have a voice in the future of the school or the library they gain a sense of **personal identity** and value.
- See how librarians and teachers use social networks appropriately they are presented with positive **role models**.

- A high school student creates a My Space site for a British poet she needs to study. As she gathers information, she enters it into the poet's My Space profile. She uses the blog function to post the poems she analyzes. Before long, other MySpace authors and poets befriend her poet. They comment on what is written and lead the student to more resources. The student has to adopt the persona of her poet and imagine what the poet's responses might actually be.

- An author creates a My Space account as a way to keep in touch with teen readers. The author's space includes biographical information, book information, and reflections on reading and writing. Teens interested in the author can communicate with him or her via My Space and are able to perform primary source research via the author's My Space site.
  See Rachel Cohn,
  http://www.myspace.com/rachel_cohn

- A public library invites parents and teens to a meeting about My Space and other social networking tools. Librarians and teachers talk about how My Space is being used in the classroom and library. Law enforcement officials are on hand to talk about how to help teens stay safe while participating in social networking online. Parents and teens leave the meeting with knowledge of what the tools are and how to use them smartly and safely.



yalsa
Young Adult Library
Services Association

More Information on Social Networking & Teens in Schools & Libraries

Farnham, Kevin and Dale. **My Space Safety: 51 Tips for Parents and Teens**. How To Primers.com, 2006.
Two parents discuss how other parents can help guarantee their teens are safe when using social networking technologies.

Prensky, Marc. **Adopt and Adapt**. Edutopia, 2005. Available at:
http://www.edutopia.org/magazine/ed1article.php?id=Art_1423&issue=dec_05#
Prensky covers why it's important for schools to integrate new technologies into the classroom.

Prensky, Marc. **Engage Me or Enrage Me: What Today's Learners Demand**. Educause, September/October 2005. Available at: http://www.educause.edu/ir/library/pdf/erm0553.pdf
A look at why using technologies that are of interest to students improves learning and engagement.

Richardson, Will. **Blogs, Wikis, Podcasts and Other Powerful Web Tools for the Classroom.** Corwin Press, 2006.
Richardson explains how and why social networking technologies can be used in the library and classroom.

Social Networking Sites: Safety Tips for Tweens and Teens
http://www.ftc.gov/bcp/edu/pubs/consumer/tech/tec14.htm
A short and useful list of reminders for staying safe on social networking sites (and online in general.) Includes a list of resources for finding out more.

Teens Content Creators and Consumers
http://www.pewinternet.org/PPF/r/166/report_display.asp
This Pew Internet in American Life report how and why teens use technology to communicate and develop content.

Weblogg-ed
http://www.weblogg-ed.com/
Educator and technology specialist Will Richardson discusses how and why new technologies should be integrated into the classroom and library on his frequently updated blog.

Wired Safety.org: Blog Sites, Profile Sites, Diary Sites or Social Networking Sites
http://www.wiredsafety.org/internet101/blogs.html
Information on what parents need to do in order to help their children stay safe when using social networking technologies.

YALSA is the fastest growing division of the American Library Association (ALA). For nearly 50 years, YALSA has been the world leader in recommending reading, listening and viewing for teens. Visit the YALSA blog at http://blogs.ala.org/yalsa.php. For more information visit www.ala.org/yalsa, email yalsa@ala.org or call 800-545-2433, ext. 4390

MS. YOKE. Chairman Upton and members of the subcommittee, thank you for inviting me to testify on behalf of the American Library Association. I sincerely appreciate the chance to comment on the Deleting of Online Predators Act.

My name is Beth Yoke, and I am Executive Director of the Young Adult Library Association, the division in ALA that strives to ensure the Nation's teens have access to excellent library service and resources.

Before taking this position with ALA, I was a young adult librarian and instructor of future school instructors in Fairmont, West Virginia.

I would like to summarize our main points. But first let me say that no one is more concerned with the safety of children online than librarians, especially youth librarians, media specialists like those with whom I work. Librarians believe, and, more importantly, know from experience that education about safe Internet practices for both youth and parents is the best way to protect young people.

With that in mind, let me go through our key points.

First, the technology used in DOPA is overly broad. DOPA uses the term "social networking sites" to describe virtually all interactive Web applications in which users converse or interact with each other. As written, it would block access to many valuable websites that utilize this type of communication, websites whose benefits far outweigh their detriments.

Second, DOPA ignores the value of interactive Web applications. New Internet Web applications for collaboration, business and learning are becoming increasingly important, and young people must be prepared to thrive in a work atmosphere with meetings that take place online and online networks are essential communications tools.

A number of businesses are increasingly leaning to the use of interactive Web applications as a primary mode of business communication. This is exactly what kids must be ready for: a professional environment where only the Web-savvy thrive.

Finally, one example that wasn't included in my written testimony. A young adult with whom I recently spoke told me, quote, "My dad is a truck driver. And before social networking sites existed, it was hard for him to feel connected with our family when he was away. If the library blocks social networking sites, I will no longer be able to have live chats with him by computer, to share photos with him, or share moments across the country." No doubt thousands of other teens have equally compelling stories to tell.

Third, education, not laws blocking access to social networking access is the key to safe use of the Internet. Librarians and schools--

MR. UPTON. We will freeze the clock. We will let you finish.

MS. YOKE. Libraries and schools are where kids learn education. Legislation like DOPA sends the wrong message at the wrong time.

MR. UPTON. It means we could have a series of votes but it is likely we are going to have one. Go ahead.

MS. YOKE. Instead of allowing librarians and teachers to instruct students about how to use all kinds of applications safely and effectively, it creates barriers to information, literacy instruction. This flies in the face of logic and hundreds of years of educational theory. Why would we limit access to interactive Web application in the first place where students came to use them actively?

Fourth, local decision-making is the way to address the law. Many of the problems that DOPA seeks to remedy are already addressed at the local level. Federal legislation like DOPA robs education communities of control. Decisions, about what is best for an individual community is best made by the community itself.

Fifth, DOPA would restrict technology in the communities that need public access most. According to research, African Americans and Hispanics are much more likely to rely exclusively on the library computer for Internet access than are their white and Asian counterparts. DOPA, as presently drafted, would require libraries and schools receiving E-rate discount to block computer users from accessing interactive Web actions of all kinds, thereby limiting opportunity for those who do not have Internet access at home.

Research shows that use of the Internet is used to improve reading and other academic successes, but as Bruce Bower states, "children most likely to benefit from home Internet access are the least likely to have it."

The American Library Association would like to affirm the importance of online interaction and collaboration as an indispensable tool for education and communication in today's information society. They also affirm the role of social networking sites of essential literacy skills. We at the American Library Association stand ready to work with you to assure that our children are protected, educated, informed and made as safe as possible.

Thank you.

[The prepared statement of Beth Yoke follows:]

PREPARED STATEMENT OF BETH YOKE, EXECUTIVE DIRECTOR, ALA YOUNG ADULT LIBRARY SERVICES ASSOCIATION

Librarians believe, and more importantly know from experience, that education about safe Internet practices – for both youth *and* parents – is the best way to protect young people. We believe that the overly broad technological controls that would be required under DOPA are often ineffective given the fast-moving nature of modern technology. Further, such technological controls often inadvertently obstruct access to beneficial sites. In essence, we believe that this legislation would lead to the blocking of essential and beneficial Interactive Web applications and would further widen the digital divide.

I. The terminology used in DOPA is flawed.

DOPA uses the term "social networking sites" in an overly-broad way to describe virtually all Interactive Web applications in which users converse or interact with each other. As written, HR 5319 would block access to many valuable applications.

II. DOPA ignores the value of Interactive Web applications.

New Internet-based applications for collaboration, business and learning are becoming increasingly important, and young people must be prepared to thrive in a work atmosphere where meetings take place online, where online networks are essential communication tools.

III. Education, not laws blocking access, is the key to safe use of the Internet.

Libraries and schools are where kids learn essential information literacy skills that go far beyond computer instruction and web searching to include the development of critical thinking skills necessary to make good choices online.

IV. Local decision-making – not federal law – is the way to solve the problems addressed by DOPA.

Many of the problems that DOPA seeks to remedy are already addressed at the local level. Decisions about what is best for an individual community should be made by the community itself.

V. DOPA would restrict access to technology in the communities that need public access most.

African Americans and Hispanics are much more likely to rely exclusively on the library computer for Internet access than are their white and Asian counterparts. DOPA, as presently drafted, would require libraries and schools receiving E-rate discounts through the Universal Service Program to block computer users from accessing Interactive Web applications of all kinds, thereby limiting opportunities for those who do not have Internet access at home.

Chairman Upton and Members of the Subcommittee, thank you for inviting me today to testify on behalf of the American Library Association (ALA). I sincerely appreciate the opportunity to comment on H.R. 5319, the Deleting Online Predators Act (DOPA). ALA has three primary concerns about DOPA: 1) that the broad scope of this legislation will limit access to essential Interactive Web applications; 2) that the legislation would widen the digital divide by limiting access for people who use library and school computers as their primary conduits to the Internet; and 3) that education and parental involvement are and have always been the best tools to keep kids safe online and to ensure that they can make the right decisions.

I am the Executive Director of ALA's Young Adult Library Services Association (YALSA). The American Library Association is the oldest and largest library association in the world with some 65,000 members, primarily school, public, academic, and some special librarians, but also trustees, publishers, and friends of libraries. The Association's mission is to provide leadership or the development, promotion, and improvement of library and information services and the profession of librarianship in order to enhance learning and ensure access to information for all.

Before taking this position with ALA, I was a young adult services librarian and an instructor of future school library media specialists and youth librarians at West Virginia University. I can say with authority that no one is more concerned with the safety of children online than librarians – especially youth librarians.

Youth librarians believe, and more importantly know from experience, that education about safe Internet practices – for both youth *and* parents – is the best way to protect young people. We believe that the overly broad technological controls that would be required under DOPA are often ineffective given the fast-moving nature of modern technology. Further, such technological controls often inadvertently obstruct access to beneficial sites. In essence, we believe that this legislation will lead to the blocking of essential and beneficial Interactive Web applications and will further widen the digital divide.

The terminology used in DOPA is flawed.

It is very difficult to define many of the terms used in the debate over Internet usage. DOPA uses the term “social networking sites” in an overly-broad way to describe virtually all Interactive Web applications in which users converse or interact with each other. As it is currently written, the definition (even with the educational exemption) would include: educational tools used to provide distance education, community forums that allow children to discuss issues of importance, online email programs through which family members can communicate with each other and with teachers and librarians at their local schools and libraries and even find one another in cases of emergency. There is enormous value to be found in these interactive online environments. Blocking access to them denies young people the opportunity to benefit from all the Internet has to offer while not necessarily ensuring kids’ safety online. As written, HR 5319 is simply too broad and would block access to many valuable applications. We urge you to consider changes in the bill language.

There are many examples of online education applications that would be blocked under DOPA. One example reported in *Education Week* indicated that more than 10 million students were part of an online field trip to the Carlsbad Caverns National Park in Carlsbad, N.M. — without leaving their classrooms.

The April 25 field trip, coordinated by Ball State University in Muncie, Ind., was to consist of two live virtual tours of the cave featuring scientists, park guides, and First Lady Laura Bush. Students in grades 3-8 were invited to call in or e-mail questions to be answered on the air, or to participate in an online discussion during the 90-minute broadcasts. The organizers billed the event as the largest simultaneous visit ever to a national park. It was also described as the largest “electronic field trip” ever broadcast by BSU, which has organized more than 50 such trips since 1996.[1]

Use of the site WebCT.com, an online education application, has helped thousands of people get their degrees through distance learning. WebCT is a site that allows users to enroll in and participate in classes online. It can also act as a forum for class discussions. Users create profiles and become students in a virtual classroom through online bulletin boards, real-time chat, student blogs, and more. In the rural areas of states like Texas, Wyoming, the Upper Peninsula of Michigan and West Virginia – where I worked, distance from major hubs once created an enormous barrier to learning.

Today, applications, like those available through WebCT, make it possible for young adults to complete degrees online at schools that are hundreds of miles away as well as access other non-credit courses for personal interests. It is our analysis that DOPA would make this type of distance learning impossible, since the bill requires that interactive applications, like courses available through WebCT, can only be used in libraries or schools if there is adult supervision. But what does “adult supervision” mean? Or how is “education” defined in the pertinent exemption? Is it formal for-credit only courses? And, why would we create barriers for young people who want to take advantage of online educational opportunities?

There are countless positive uses for networking applications that are not necessarily related to formal education. Networking applications include support groups for teenagers with physical or emotional disabilities, forums for the exchange of ideas, and even tools to help kids become acclimated to new surroundings. For example, when teenagers leave for college they often use networking sites to find other students with similar interests.

[1] Tonn, Jessica. “Expert Sees Need for School Staff To Access Social-Networking.” *Education Week*. Vol. 25 Issue 33, p16.

Finally, with specific regard to “social networking sites,” young adults all over the country have begun to use these sites as a primary means of communication, whether with their peers or with young adult authors, musicians, artists, and with libraries. Some libraries are taking advantage of this by using some of these sites to stay in touch with their communities. For example, Sean Rapacki from the Wadsworth Public Library in Wadsworth, Ohio informed us that his staff has created a MySpace profile page FOR the library, allowing library staff to communicate with young adult patrons much more effectively.

DOPA ignores the value of Interactive Web applications.

Today's interactive online environment is an essential and growing part of economic, cultural, civic, and social life. New Internet-based applications for collaboration, business and learning are becoming increasingly important, and learning to use the online environment effectively and safely is now an essential component of education.

The popularity of interactive online environments is extending to the corporate world, as a number of businesses – including corporate leaders like Ernst & Young and IBM – are increasingly moving to the use of interactive Web applications as a primary mode of business communication. These companies recognize that technology can be an essential way to achieve a home/work balance and maximize efficiency.[2] As the corporate, professional, and civic use of interactive Web applications grows, there is an increasing need for today's young people to be prepared to thrive in a work atmosphere where meetings take place online, where e-business is a driving force behind the world economy, and where online networks are essential communication tools. This is exactly what kids must be ready for: a professional environment where only the web-savvy thrive.

The Internet is changing how we live, learn, work, and interact with one another. If today’s young people are to succeed in the workplace of the future, they must learn information literacy skills for the technologies of today and tomorrow. Libraries are far and away the best places to learn these skills, and social networking sites, which *introduce* kids to the world of online interaction, are key to successful development in that field.

Education, not laws blocking access, is the key to safe use of the Internet.

Libraries and schools are the locations where students develop the information literacy skills that are vital to success in today's world. Information literacy includes “the abilities to recognize when information is needed and to locate, evaluate, effectively use, and communicate information in its various formats.[3]“ These are skills that public librarians and school library media specialists are in a unique position to foster in young people. In today’s world, information literacy skills go far beyond computer instruction and web searching. In a fully developed information literacy program, students learn how to find, evaluate, and use online information and also learn how to use critical thinking skills to make good choices online.

This type of information literacy instruction is going on in schools and libraries all across the country. Legislation like DOPA sends exactly the wrong message at the wrong time – instead of allowing librarians and teachers to instruct students about how to use all kinds of applications safely and effectively, it creates barriers to information literacy instruction. This flies in the face of hundreds of years of educational theory – why would you limit access to interactive Web applications in the one place where students can learn to use them safely?

[2] “Life Beyond Pay-Work-Life Balance,” *The Economist,* July 7, 2006.

[3] *Information Literacy: Skills for the Information Age*. Westport: Libraries Unlimited. Page 5.

Fortunately, thousands of public and school libraries across the country, along with websites like Ms. Aftab's WiredKids.org, are doing an outstanding job in helping parents teach children how to use the Internet safely and responsibly. For example, Baltimore County Public Schools and the Baltimore County Public Library co-sponsored a *Family Guide to Child Safety on the Internet*, a valuable resource for helping parents teach their kids the do's and don'ts of web surfing.[4]

Local decision-making – not federal law – is the way to solve the problems addressed by DOPA.

As advocates for effective use of information, librarians and teachers are fully committed to helping young people have safe online experiences; furthermore, we teach young people the information literacy and critical thinking skills they need to use the Internet safely and effectively. We reach the goal of educating kids to safely use online tools with information literacy education programs as described above, and through locally-developed online safety policies, which in many cases include the use of technological barriers like filters. In other words, many of the problems that DOPA seeks to remedy are already addressed at the local level.

About 80% of all public library funding is local, library programs are developed to be responsive to local requests, and the policies governing libraries are developed with local trustees and community members; comparable policy decisions are made by school boards. Federal legislation like DOPA robs libraries and communities of local decision-making and control. Decisions about what is best for an individual community should be made by the community itself.

DOPA would restrict access to technology in the communities that need public access most.

According to recent statistics from the U.S. Census Bureau the digital divide is large and does not appear to be shrinking. Currently, roughly one out of seven African Americans and only one out of eight Hispanics subscribe to broadband service at home. Meanwhile, 26.1% of whites and a full one third of Asians have broadband at home.[5] Further, according to a Gates Foundation report on the role of libraries in Internet access, African Americans and Hispanics "rely exclusively on the library computer for Internet access to a greater degree than their white and Asian counterparts," with approximately a fifth of African American users and nearly 16% of Hispanic users exclusively relying on library-based computers. Also, nearly a third of those in the lowest income bracket who use library computers rely exclusively on them.[6] These data indicate that public access computing in libraries is playing an important role in closing the digital divide.

Since DOPA, as presently drafted, would require libraries and schools receiving E-rate discounts through the Universal Service Program to block computer users from accessing Interactive Web applications of all kinds, opportunities for those who do not have Internet access at home would be further limited.

There is a great deal of research being conducted on young people and their use of the Internet and interactive applications. There is much to learn from this research about educating young people and helping them to safely use the Internet. For instance, research shows that use of the Internet, including interactive sites, leads to improved reading and other academic successes. Sadly, research reported by Bruce Bower

[4] http://www.bcps.org/offices/lis/

[5] http://www.census.gov/prod/2005pubs/p23-208.pdf

[6] *Toward Equality of Access: The Role of Public Libraries in Addressing the Digital Divide*. Pages 19-20. http://www.gatesfoundation.org.

indicates that "children most likely to benefit from home Internet access are the very children least likely to have [it]."[7]

The ALA would like to affirm the importance of online interaction and collaboration and the development of essential information literacy skills. We at ALA stand ready to work with you, to assure that our children are protected, educated, informed and made as safe as possible.

Biography for Beth Yoke

Beth Yoke earned a B.A. in History from Gettysburg College in 1991, a teaching certificate from Tulane University in 1995 and a Masters in Library and Information Science from Louisiana State University in 1998. From 1991-1993 she taught in Orleans Parish Schools, New Orleans, LA, as a member of the Teach for America corps. From 1993-1997 she continued her teaching career in Orleans Parish Schools. While pursuing her masters in Library and Information Science, Yoke worked at in the research and development library for Albemarle Corporation in Baton Rouge, LA. After completing graduate school, Yoke worked as a high school librarian in Stafford, VA then as a university librarian at Fairmont State University in Fairmont, WV. At Fairmont State Yoke coordinated the online school library media certification program and became active in the West Virginia Library Association, where she served as first as chair of the School Library Division and later as WVLA's Second Vice-President. Since 2004 Yoke has served as Executive Director of the Young Adult Library Services Association (YALSA), the fastest growing division of the American Library Association.

MR. UPTON. Mr. Zellis, we will hopefully conclude with you and we will break and go vote, so go ahead.

MR. ZELLIS. Chairman Upton and members of the committee, ladies and gentlemen, thank you for the opportunity to be here today to talk about the serious issue that affects our most treasured resource, our children, and our efforts to protect them from the dangers of social networking sites that exist on the World Wide Web.

My name is David Zellis and I am the highest-ranking prosecutor next to the elected district attorney in Bucks County. I have spent the last 22 years fighting in the courtroom to put criminals behind bars. My courtroom experience involves every type of case including capital murder. I also worked hand in hand with law enforcement as they investigated criminal activities. One could say that during my tenure as a county prosecutor I have seen it all. Despite my exposure to all kinds of criminal behavior, I, like many of my colleagues, have been shocked and dismayed by the latest rage, politely known as social networking sites, but commonly known as MySpace, Friendster, Facebook, and Xanga.

It was not many years ago the police arrested and I prosecuted child molesters for making advances toward our children on the street corner or some park. It was not that long ago the drug dealing took place on the street corners and I locked those drug dealers up. And it was only a short time ago that bullying meant beating up a kid on the playground.

[7] "Growing Up Online," *Science News*, Vol. 169 Issue 24, p376.

Times have changed. The Internet and these social networking sites have redefined, reinvented, and reinvigorated child predators, drug dealers, and bullies. Now sexual predators troll the social networking sites rather than the streets and get all of the information they need in order to groom children for the ultimate purpose of victimizing them. Drug dealers in suburban communities like Bucks County can now conduct business in cyber space instead of on the street corner, and bullies do not have to throw a punch when they can go on the Internet and engage in cyber bullying and inflict more pain and suffering on kids than a night on the school yards used to cause.

Bucks County, Pennsylvania is a diverse northern suburb or Philadelphia--

MR. UPTON. Keep going.

MR. ZELLIS.--with over 600,000 residents. It represents a typical suburban community. We have areas where crime is higher than other areas, but on the whole, the streets of Buck County are very safe. The Information Superhighway, however, poses a significant challenge to law enforcement, schools, parents, and legislators as we try to balance the benefits and the dangers that lurk in cyberspace.

There are four recent cases that occurred in Bucks County that poignantly illustrate the dangers posed by such sites as MySpace. In the first case, a 14-year-old boy had his profile posted on MySpace. In April of 2006 he was contacted by a male posing as a teenager, who convinced the 14-year-old to lie to his mother and have her drop him off at the local mall. The male met the 14-year-old at the mall and then took him to a motel where he had sexual intercourse with the child. This scenario has happened on a number of occasions and was only discovered when a school official overheard the 14-year-old's conversation with a friend and reported it to law enforcement.

Following the arrests, the male perpetrator was identified as a 25-year-old. The 14-year-old who had never been in trouble before and prior to this had no sexual experience. The sexual predator now sits in the Bucks County prison awaiting trial.

The next case is one of the first cases in which law enforcement arrested someone for selling drugs on MySpace. Not only was this juvenile selling drugs on MySpace but he was pictured on MySpace with an assortment of guns.

The third case involves a 13-year-old girl who posted her pictures on MySpace. A male began conversing with her on the Internet. Fortunately, the child's mother contacted law enforcement and the police took over the conversations with this sexual predator and ultimately arrested him. He was identified as a male who was working in an OB-GYN office.

Finally, we have seen street gangs taking advantage of the opportunities provided through social networking sites, and such street gangs as the Bloods and the Crips used the site's social networking recruitment tools in the suburbs. Too often as a society we think that sexual predators' Internet crime is somebody else's problem, not ours. Those of us in law enforcement know that nothing could be further from the truth.

These four examples within the last 6 months indicate the kinds of criminal activity in cyber space know no boundaries and now happens on a national/international level. My office is not only prosecuting such cases in court, but we are proactively engaged in prevention activities. We have gone into the elementary, middle, and high schools to educate students about the dangers involved in social networking sites. We have held town meetings around the county about how to keep their children safe on the Internet. These programs have been well received by students and parents and it has become clear to us that parents and most kids do not want pornography or sexual propositions to interfere with their use of the Internet.

During the course of our town meetings with parents, we have found a hunger on the part of parents to learn as much as they possibly can, because parents legitimately feel they are playing catch-up to their children when it comes to the Internet. One of the critical components of the Deleting Online Predators Act is requiring the Federal Trade Commission to create a website which can be used as a resource for parents, teachers, and others regarding the dangers on the Internet to child users.

In addition, to require that the Federal Trade Commission issue alerts is critical to providing parents and teachers with worthwhile information that they crave.

This begins to address one of the most significant concerns, and that is that no one is controlling the Information Highway.

Finally with respect to the Deleting Online Predators Act, if you knew that a child molester was going to the library or to the school and grooming children for future sexual exploitation, would you allow such behavior to go on? Of course not. But that is exactly what is going on when children in the school or at the library are permitted to freely access commercial networking sites like MySpace and chat rooms while sexual predators lurk in their midst on cyber space. We cannot and should not permit our children to fall prey to the exploits of sexual predators while they are at school or at the library. We have seen firsthand that when law enforcement officers pose as a teenager online, sexually explicit instant messaging and solicitation occur quickly and rampantly. There can be no doubt that a child's innocence, and perhaps even more, can be lost in an incident on the Internet.

On behalf of Bucks County, we endorse the act because it educates parents and children about the dangers of the Internet and limits access to certain sites during the school days. Our children's safety must come first.

[The prepared statement of David W. Zellis follows:]

PREPARED STATEMENT OF DAVID W. ZELLIS, FIRST ASSISTANT DISTRICT ATTORNEY, OFFICE OF THE BUCKS COUNTY DISTRICT ATTORNEY, COMMONWEALTH OF PENNSYLVANIA

Chairman Upton, members of the committee, ladies and gentlemen. Thank you for the opportunity to be here today to talk about a serious issue that affects our most treasured resource, our children, and our effort to protect them from the dangers of "social networking sites" that exist on the World Wide Web.

As the highest ranking prosecutor next to the elected District Attorney, I have spent the past twenty-two (22) years fighting in the courtroom to put criminals behind bars. My courtroom experience involves every type of case, including capital murder. I also work hand in hand with law enforcement as they investigate criminal activity. One could say that during my tenure as a county prosecutor "I have seen it all". Despite my exposure to all kinds of criminal behavior, I, like many of my colleagues, have been shocked and dismayed by the latest rage, politely known as "social networking sites", but commonly known as MySpace, Friendster, Facebook and Xanga.

It was not that many years ago that police arrested and I prosecuted child molesters for making advances toward children on the street corner or in the park. It was not that long ago that drug dealing took place on the street corners, and I locked those dealers up, and it was only a short time ago that "bullying" meant beating up a kid on the playground. Times have changed. The internet and these social networking sites have redefined, reinvented and reinvigorated child predators, drug dealers and bullies. Now sexual predators troll the social networking sites rather than the streets, and get all the information they need in order to groom children for the ultimate purpose of victimizing them. Drug dealers in suburban communities like Bucks County can now conduct business in cyberspace instead of the street corner. And bullies do not have to throw a punch when they can go on the internet and engage in cyber bullying and inflict more pain and suffering on kids than a fight in the school yard used to cause.

Bucks County, Pennsylvania, is a diverse northern suburb of Philadelphia. With over 600,000 residents, in many ways it represents a typical suburban community. We have areas where crime is higher than other areas, but on the whole the streets of Bucks County are very safe. The information superhighway, however, possesses a significant challenge to law enforcement, schools, parents and legislators, as we try to balance the benefits and the dangers that lurk in cyberspace.

There are four recent cases that occurred in Bucks County that poignantly illustrate the dangers posed by such sites as MySpace. In the first case, a fourteen year old boy had his profile posted on MySpace. In April of 2006 he was contacted by a male posing as a teenager, who convinced the fourteen year old to lie to this mother and have her drop him off at the local mall. The male met the fourteen year old at the mall and then took him to a motel, where he had sexual intercourse with the child. This scenario happened on a number of occasions, and was only discovered when a school official overheard the fourteen year old's conversation with a friend, and reported it to law enforcement. Following the arrest, the male perpetrator was identified as a twenty-five year old. The fourteen year old had never been in trouble before, and prior to this had had no sexual experience. The sexual predator now sits in the Bucks County Prison awaiting trial.

The next case is one of the first cases in which law enforcement arrested someone for selling drugs on MySpace. Not only was this juvenile selling drugs on MySpace, but he was pictured on MySpace with an assortment of guns.

The third case involves a thirteen year old girl who posted her pictures on MySpace. A male began conversing with her on the internet. Fortunately, the child's mother contacted law enforcement and the police took over the conversations with this sexual predator and ultimately arrested him. He was identified as a male who was working in an OB/GYN office.

Finally, we have seen street gangs taking advantage of the opportunities provided through social networking sites, and such street gangs as the Bloods and Crips use the sites as a recruitment tool in the suburbs.

Too often as a society we think that sexual predators and internet crime is somebody else's problem, not ours. Those of us in law enforcement know that nothing could be further from the truth. These four examples which occurred in Bucks County within the last six months indicate that the kind of criminal activity in cyberspace knows no boundaries, and now happens on a national and international level.

My office is not only prosecuting such cases in court, but we are proactively engaged in prevention activities. We have gone into elementary, middle and high schools to educate students about the dangers involved in social networking sites. We have held town meetings around the county to educate parents about how to keep their children safe on the internet. These programs have been well received by students and parents, and it has become clear to us that parents and most kids do not want pornography or sexual propositions to interfere with their use of the internet

During the course of our town meetings with parents, we have found a hunger on the part of the parents to learn as much as they possibly can, because parents legitimately feel that they are playing "catch up" to their children when it comes to the internet. One of the critical components of the Deleting Online Predators Act is requiring the Federal Trade Commission to create a website which can be used as a resource for parents, teachers and others regarding the dangers on the internet to child users. In addition, the requirement that the Federal Trade Commission issue consumer alerts to parents and other regarding the potential dangers of internet child predators is critical to providing parents and teachers with worthwhile information that they crave. This begins to address one of the most significant concerns, and that is that no one is controlling the information highway.

Finally, with respect to the Deleting Online Predators Act, if you knew that a child molester was going to the library or to a school and grooming children for future sexual exploitation, would you allow such behavior to go on? Of course not. But that is exactly what is going on when children in school or at the library are permitted to freely access commercial networking sites like MySpace and chat rooms, while sexual predators lurk in their midst in cyberspace.

We cannot and should not permit our children to fall prey to the exploit of sexual predators while they are at school or at the library. We have seen first hand that when a law enforcement officer poses as a teenager on line, sexually explicit instant messaging and solicitations occur quickly and rampantly. There can be no doubt that a child's innocence and perhaps even more can be lost in an instant on the internet.

On behalf of Bucks County District Attorney Diane E. Gibbons, we wholeheartedly endorse the Deleting Online Predators Act because it educates parents and children about the dangers of the Internet and limits access to certain sites during the school day. Our children's safety must come first.

MR. UPTON. Thank you. I am going to have to stop. We have less than 5 minutes to go on this vote. We will come back about 12:15.

[Recess.]

MR. FERGUSON. [Presiding] Chairman Upton will return shortly. I had some questions for the Attorney General but I don't see him. I know he has to go at some point. So I wanted to make sure we got to him first.

I am going to start with Mr. Zellis. We appreciate you being here today, and all of our witnesses. How much of an impact do you believe that limiting access to social networking sites and chat rooms at schools and/or libraries would have in terms of the crimes you see in your own experience in Bucks County?

MR. ZELLIS. It is very hard to say. If we could save one child then it is worth it, because that one child, that innocent child who may fall prey during the school hours or at a public school to a sexual predator because the legislation wasn't enacted, would just be a catastrophe for that child, for that family, and for that child for the rest of his or her life.

MR. FERGUSON. But in terms of your own experience, it is tough to say with specificity as to how this legislation might be able to assist you in catching some of these folks.

MR. ZELLIS. I did check around my office before coming down today to --

MR. FERGUSON. Keeping it from happening.

MR. ZELLIS. And we are not aware of any case to date in our jurisdiction that involves a child falling prey as a result of being online at school or in the library. But that could change this afternoon. That could change tomorrow. This is an evolving problem in our community.

MR. FERGUSON. Thank you.

Mr. Attorney General, thank you again for being with us here today. How aware do you find that parents are with regard to the content and the potential danger at these sites? Clearly kids are ahead of parents many times when it comes to new technology. Do you find that parents at this point are doing a good enough job, or how widespread is the problem of kids being ahead of their parents with regard to this technology, particularly with these social networking sites?

MR. ABBOTT. Let me fully answer that, if you don't mind, if I could follow up and add on to the last comment. And I came in maybe after the question was already asked, but my perception was any of these kids who are assaulted online, at school, then go out and get assaulted. I may not have perceived that correctly. But here is the deal of where that would typically work. They would be online on one of these social networking sites at school or at home. They will chat perhaps for days before they will eventually decide to go ahead and make the decision, yeah, I can trust this other 14-year-old boy. I will show up at the mall and meet him.

It is not something that typically happens like that. They chat for 5 minutes at school. Meet you after school, for someone they have never met before. So the school location would be one of several different locations. School, home, and maybe a friend’s house. These children will chat for a while before they will eventually make the decision to show up and wind up getting assaulted.

MR. FERGUSON. So in terms of the legislation, if you close off one of those opportunities, perhaps it will have some impact. Is that what you are saying? I was asking about the bill that we are talking about today in terms of schools and libraries.

MR. ABBOTT. The reality is, if you close off one opportunity, it doesn’t mean that children will not access the networking websites. It means they will do it at home or do it at a friend’s house, someplace other than schools. So shutting it down at school--put it this way. Putting restrictions on children’s access to this, putting things like age verification in there, things like that will all be steps in the right direction. But if the goal is to shut it down at one place and pretend that that is going to solve the whole problem, that probably won’t achieve a whole lot because kids go to friends’ houses or homes or wherever else, perhaps in an unsupervised situation, and wind up getting caught in the same bad scenario.

But I would think that limitations on access, age verification, like we have talked about before, to ensure that children for one are not going to be subjected to pornographic or otherwise age material, other kind of restrictions would be helpful for children.

But if I could, let me address your question about education because we find that parents are woefully uneducated about this. They feel like they are not up to speed. Like was testified earlier, we have put on several town hall meetings where we have seen literally hundreds of parents come in to one meeting and they are absorbing this information as quickly as possible, eager to learn everything they possibly can to find ways that they can do something to help protect the children.

And I will tell you this: It kind of demonstrates exactly where a parent stands on this. What we do when we put on our town hall meetings, we tell parents about the problem. We go into it and all that kind of stuff, and about 15 minutes through the presentation we log onto MySpace and we plug in only the school where we are putting on the town hall presentation or only the zip code that we are in, and we put in only an age bracket of about 2 years that would include juniors and seniors; and all of a sudden these pictures come up; pictures and names that parents recognize and students recognize, and you can hear audible gasps in the audience about parents not realizing that their children are on these websites. Sometimes very provocative pictures, and parents are aghast at what is going on.

So they are pretty much--some parents are completely unaware. Some of them--many people have heard about MySpace now, but don't know what it does. They need a vast amount of information quickly to help protect their children. One thing--I know you want to ask a question, if I can make this one key point.

MR. FERGUSON. I know your time is short but my time is short. I have a more specific question about language in the bill.

Some have raised concerns about language in the bill about this prohibiting minors from being able to easily access--and those are words from the bill--easily access obscene content or otherwise easily be approached by predators online. In your written testimony, you had raised some concerns with this language. You didn't mention it in your verbal testimony. Can you expand a little bit on your thoughts on the language "easily access"?

MR. ABBOTT. As a lawyer who litigates cases in court, as a former judge, I believe the word "easily" would be categorized as vague. It is hard to know exactly what that means. Frankly, I can't tell you what it means. And if we had 12 different jurors we could have 12 different decisions about what it means.

Now, the position I would advocate probably would be one different than some other folks on this panel. I think an easy solution for it is to delete the word "easily," so that it just goes straight to "access." But the word "easily" is potentially vague, and here is what would wind up happening if the bill passed with this current language. We would all spend years in court litigating what "easily" means, and the evidence will be put on, no, we are not easily accessible and the evidence would be put on, yes, you are. So it would lead to litigation that would frustrate implementation of the bill.

MR. FERGUSON. I recognize Ms. Eshoo for questions.

MS. ESHOO. Thank you, Mr. Chairman. I want to thank all of the panel. I have learned a great deal from listening to you this morning--from law enforcement, Attorney General, and Mr. Zellis; the horror of what is taking place. And I certainly want to salute you for the work that you are doing to bring these predators to justice. To all of the other panelists, thank you.

Ms. Aftab, it seems to me a lifetime of work that you are doing. Mr. Davis, I think that you have really offered a solid model of how to address this, and I want to thank you for your work. To Chris Kelly and the work that you are doing, which I think really is the model for any social networking operation, the work that you are doing and that they all have someone like you. We need to clone you. To the Pew Center, and I think what you have put out should be kept in the top drawer of everyone's desk here because it is unbiased, solid information about how everything works. To the libraries, who are absolutely terrific.

Now it seems to me that the intention of the authors of the legislation is really very good but it is really not the prescription to handle this.

The language in the bill as I see it, on page 2, I think it is line 24, "may easily access or be presented with obscene or indecent material," I don't really know what that means legally. And I think the Attorney General just suggested that the world "easily" be dropped.

But if we just go with "access," I think, Mr. Attorney General, we need to appreciate that Google will be completely knocked out of business in schools and libraries; Yahoo, anyone in the Internet business, is in one fell swoop going to be erased. And that is not pragmatic. That is not what we are going to do. But we are still left with the challenge of addressing this.

What I would like to press, whomever would like to come up with a prescription here, what your prescription would be. It seems to me, just off the top of my head, I think that if the Congress had actually put into place broadband for everyone in the country and we had money in it, then we could restrict the money. And that would be I think a win-win. But since we don't have a national broadband policy, that is not in the offing right now, that being able to restrict any funding that would be attached to that is not something that we are going to be exercising.

Now, having said that, knowing the language of the bill not really being workable, I mean it is again the case of the intentions are great but it is not the way we are going to resolve it.

Let me ask the law enforcement people, number one. Maybe you don't agree with me. If you don't, say so. What is your prescription for a solution to this?

MR. ABBOTT. A couple of things. And these are things that may be coming from left field with regard to these particular bills, but these are the things that we in the law enforcement field need to see and need to see from the social networking sites and basically anyone, and that is we must have better retention of IP records or logs. Literally, as we speak, records of predators are being lost and deleted. Retention periods must be extended to give law enforcement time to issue the legal processes that are needed to obtain the records for evidentiary purposes. That is for one.

For another, education has been talked about a lot as absolutely necessary. The providers of this software, the providers of these sites, can take the lead in ensuring the education is provided. They are on the site. So those would be two things.

Age verification, again, I believe would be very helpful.

MS. ESHOO. Chris, do you want to speak to this, please--

MR. KELLY. Age verification, we use kind of a proxy process for age verification in terms of associating people with an associated high school. That seems to be about as effective as we have been able to get it, as we talked about on the dialoguing. There is a lot of public record checking. But we found that the approximate e-process through the high school association is relatively good in terms of keeping in terms of keeping under-13s off the site, and that is a standard that has been set by Congress, obviously, in whether or not you need verifiable parental consent at that stage. So that for age verification, that seems to be somewhat workable for us.

But we don't have the only model in the industry and we do think that there are a number of good things facilitated by some of the other sites. I mean, we like our model the best, but we don't think the others should be outlawed.

MR. ABBOTT. If I could very briefly say one thing about their website. I don't believe that any of these sites are perfect, but I believe that the program that Facebook has created is superior. If you compare it to the real world of neighborhoods, where all of you live, you have seen so-called safe neighborhood programs. They do as well of a job as I have seen at creating safe neighborhoods, neighborhoods that are confined. And that I think is a superior approach to what we have seen elsewhere. Perhaps you can look at some aspects of their model and require those similar components to be required above the board.

But don't get me wrong; I am not going to concede your model is perfect. It is a great first step.

MS. ESHOO. I think what we have to keep in mind, Mr. Chairman, is that there isn't any such thing as good technology and bad technology. Technology is neutral in that sense. It is how it is used and how we help shape the direction of it. But we really can't go after the technology itself. This is really a sticky wicket because we have some constitutional issues involved in this as well.

So, I am over my time. Now I will stop. I really want to thank the Chairman for the hearing and for the testimony today because I find it is enhancing. So thank you.

MR. FERGUSON. Mr. Shimkus.

MR. SHIMKUS. Thank you, Mr. Chairman; and I appreciate you all coming.

This is a legislative hearing, but sometimes we digress and address things. My good friend Anna and I work on a lot of these issues together; and this is very similar, I think, to the discussions we had years ago when we started doing the actual purchasing of items and goods over the Internet, remember, with digital signatures. VeraSign was in here.

So my first--one of my questions was--Anna, you were already mentioning to Chris--was age verification; and my comment, based on listening to the testimony, is a program like VeraSign or some authentication, which has really been successful, and it was a private sector, it was technologically neutral, but it had some standards by which we could allow some current commerce to flow and identification really be taken--

I mean, how many times do we do stuff now--I mean, there is identity theft. We still have problems. I mean, we are still in a central world. There is still going to be bad guys who figure out--but for most of us, when you can do on some standards--

So you kind of addressed it, Chris, but, I mean, is that the approach that we have--is this a third-party age verification process? You can out there, in essence, do that? I mean, you shake your head, no, Parry, but we do it for commerce.

MS. AFTAB. If I may, the reason I am shaking my head no, we can do it technologically, but the kids won't buy it. So I have just finished polling 14,000 pre-teens and teens over the last 4 months in person, face to face; and they are scared. I have never seen kids scared before.

MR. SHIMKUS. These are the same kids who are going to download a piece of music for, what, 75 cents a song, 25 cents a song.

MS. AFTAB. Or for free.

MR. SHIMKUS. But probably have more discretionary income than any kids in any generation before.

MS. AFTAB. Because they are not paying for music.

But, Mr. Shimkus, what they all say to me, we want authentication. We want the site to know who everyone is.

One girl who lives on a Marine base in Yuma said the answer is to keep all boys over the age of 14 off MySpace.

MR. SHIMKUS. Let me interrupt you there. But wouldn't there then be a market?

MS. AFTAB. Yes, except--

MR. SHIMKUS. I am a market Republican, believe market principles, wouldn't someone set up a Facebook for girls?

MS. AFTAB. Well, what happens is--

MR. SHIMKUS. With authentication--I mean, we still have girl's schools. We still have guy's schools.

MS. AFTAB. The kids don't want parents involved in authentication. They don't want schools involved in authentication.

MR. SHIMKUS. They are kids. They are kids.

MS. AFTAB. You can authenticate them, but they won't go there. So they will go someplace else.

There is a model that Facebook is using which is for the school, school e-mail addresses. Xanga is now using some new models that are having kids identify each other. YFly, the new one with Nick Lachey, will do that, but the kids will go someplace else because they don't want their parents and schools to know who they are. They want the site.

MR. SHIMKUS. I do have the basic problem with the premise that kids are adults, and that brings a parenting aspect back into this. As much as we are going to push industry and individuals and government to solve this problem, it is still a parental issue.

MS. AFTAB. Yeah. I just want to be clear. I am not saying that we should let kids run it. What I am going to tell you, as much as we can set these things up, it won't work because the kids won't do it. They will just go underground someplace else tomorrow. And that is our only concern, as we have been facing this.

MR. KELLY. If I may jump in a minute.

MR. SHIMKUS. Please save me.

MR. KELLY. You want to have some means by which they are associated with the community and that enables not just the basic sort of identity verification but it has the community aspect over time of saying this person is a member of this community or not.

MR. SHIMKUS. That is what you do.

MR. KELLY. That is what we do at this point. By only allowing that to be associated with particular high schools, we have a proxy for age at that point because there just aren't many 12-year-olds or under in high schools. It is not perfect, nonetheless, but it gets the job done better than a lot of other means and, without driving kids away. So it is a balance there, as Parry articulates, between imposing a great number of burdens on kids in terms of authentication of their identity and driving them to sites that just wouldn't have anything at all.

MR. SHIMKUS. Well, and the Attorney General mentioned that you have a particular--I mean, he praised what you all do, and that may be a good model.

Again, my premise is our kids; and if we don't get them in some arena by which they can do this that is somewhat controlled then there are no controls.

MR. KELLY. Our preferred method is to validate with e-mail addresses, and we can only do that right now for 15 percent of high schools. We are constantly looking at effective non, deterring ways to get kids into validated networks in a meaningful way without driving them away.

MR. SHIMKUS. Yeah. I have three small boys, and I am watching this development. I taught high school for 4 years, and I grew up, so I am trying to remember my history of growing up versus what my kids are going through.

And when I taught psychology, talking over the phone was the way that you shared information discretely with your friends for hours--I don't want to typecast it to girls, but I think primarily it was--but they wouldn't have shared as much information if they knew it was a party line.

What the problem is, people don't understand that this is a party line, and it is huge.

Let me ask--if you know the answer, don't answer the question. I want to ask everybody. Is there a safe site for kids for information services now on the Internet? Just go from left to right.

MR. ABBOTT. For information services?

MR. SHIMKUS. For information.

MR. ABBOTT. A safe site?

MR. SHIMKUS. A safe site.

MR. ABBOTT. I don't have one at hand.

MR. SHIMKUS. Okay. Good. That is a no.

Parry, do you know the answer?

MS. AFTAB. Can I give you maybe? I mean, Toontown with Disney is interactive safely because it is a dropdown menu, but, otherwise, no. Because it is not--

MR. SHIMKUS. Okay. Next.

MS. COLLINS. Well, the National Center for Missing and Exploited Children, we actually have a website set up for kids, netsmartz.org--with a Z. It has information on safety for kids.

MR. SHIMKUS. Can you hyperlink out of it?

MS. COLLINS. Actually, we are in control of the website, so, no.

MR. SHIMKUS. Okay. That is good.

MR. DAVIS. I would vote for her site.

MR. SHIMKUS. All right.

MR. KELLY. We would never claim to be perfectly safe.

MR. SHIMKUS. The question is, is there one out there for information?

MR. KELLY. I mean, information, there are quite a number--

MR. SHIMKUS. That you can't hyperlink out once you go on the Internet to get information.

MS. AFTAB. Where people can post information safely?

MR. SHIMKUS. No, just information.

MR. KELLY. To get information safely.

MR. SHIMKUS. The librarian should have this, I hope.

MR. KELLY. Netsmartz does a fantastic job.

MR. SHIMKUS. All right. You guys are failing.

Next, next, next.

MS. LENHART. For information about online safety.

MR. SHIMKUS. Not information on online safety. For information, period.

MS. LENHART. Well, as long as there is no interactivity.

MR. SHIMKUS. Is there a site that has no interactivity?

MS. LENHART. Sure, sure.

MR. SHIMKUS. Next, next.

MS. YOKE. I very much appreciate your question.

MR. SHIMKUS. I am not setting it up for her, but I just pulled out this thing, and I have got the list.

MS. YOKE. Sure. The ALA believes that education is what will keep kids safe; and because of the fact that virtually any and every website that is out there on the Internet can link to something else and nothing can ever be 100 percent safe, leaving your house in the morning does not leave you 100 percent safe, that it is education that will help parents and kids stay safe.

Driving, for example, can be dangerous, but the solution has not been to ban teens and young adults from ever getting behind the wheel. The solution has been to provide them with things such as drivers education in high schools across the Nation. And we also--

MR. SHIMKUS. You are letting me down. There was a simpler answer for you.

MS. YOKE. We also would agree that driving on the information highway can also be dangerous. So what we need to do is give kids the skills, tools, and resources so that they can become safe and make good choices on the information highway.

MR. SHIMKUS. Okay. Next. You failed. Dagnab it. I set you up for it. Home run.

MR. ZELLIS. I am on my seat waiting for the answer.

MR. SHIMKUS. Okay. The answer is--Mr. Markey mentioned in opening statements, Attorney General, when you do your town hall meetings--I hope you mention this--especially for kids--we set it for kids under the age of 13. Now that I have kids--they are way past that, but it is good for kids 6, 7, 8, 9--www.kids.us. It is a safe site for kids for information.

Now there are over 20 users, and the American Library Association is a member: Americanlibraryassociation.kids.us. ABC.kids.us, American Library--I said that--games.kids, info.kids, connects.kids, music.kids, newyork.kids. Texas should be on here. Shimkus should be on here.

So I am taking myself--there are no hyperlinks. There are no chat rooms. It is information-based only.

My sister has just got her degree in education as a third or fourth career. I went to her class on information technology, took my 4-year-old with me; and the way my 4-year-old climbs up on the desk, he hits E for Internet Explorer and what is his default? Kids.us. Can he go anywhere from there? No. It is a safe site for kids that we passed here in legislation that it is part of my job to make information available, to talk about it because it works; and I just hope you take that back with you.

My time is way expired. Thank you.

MR. FERGUSON. The gentleman from New York, Mr. Engel, for questions.

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

My youngest child is 12, very, very bright young man, but I always tell him he is like an addict when it comes to the computer. I mean, he comes home from school, and the first thing he does is he goes down to the basement and starts with the computer, and he is not doing his homework, he is chatting or whatever, and it is just a terrible thing.

We had a bill that I am doing with the chairman which actually passed the House. It has nothing to do with this. It is a spoofing bill. And one of the things that I said was the problem is we are always playing catch-up. Because the bad guys are doing things and then we find out about it and then we play catch-up to try to thwart them.

It is very similar here. I think the bill is fine. Targeting schools and libraries as a condition of E-rate funding is fine, but I think that it is only a very small, little part. I guess we have to start somewhere, but I think the bill really doesn't solve the problem. Because, just as our children are the first generation to grow up with the personal computer, we are the first generation of parents to be raising children with these computers. So the whole thing is frustrating.

I am thinking, why aren't we doing a massive education campaign for parents to learn how to protect their children in the online world? I mean, I am so far behind my children it is really almost a joke.

Mr. Shimkus talks about his 4-year-old, well, my 12-year-old is my youngest; and he can just run circles around me. When I get stuck on the computer, I call him and he--oh, dad, all you need to do is this.

So, Ms. Aftab, in your written testimony you say, while this may appear on its face to be an easy answer, it is neither easy nor the answer. And I agree with you. I pulled that out because I thought that I would agree with you.

So I don't know what to say. I want to just give you an opportunity to expand on that, because I think that sort of sums up the way I feel. And I have a couple of questions if anyone else would care to answer.

MS. AFTAB. Thank you very much, Mr. Engel.

I think that everyone is worried. Law enforcement is worried, regulators are worried, legislators are worried, parents are worried, schools are worried, kids are worried. We have to do something.

It sounds easy to turn around and say the one thing we can control, schools and libraries, through the E-rate, turn it off. But since all of the social networks, the social network technologies are going to be used by all of the ISPs, by all of the big sites, by Disney and Viacom and everybody else, it is the future of the Internet. This is where everything is going. So we would be turning off, effectively, the entire Internet with this, number one.

Number two, it is not really addressing the issue. The kids, when they are involved with sexual predators, require grooming time. It is hard to do that in the library when everyone is fighting for a computer or in the classroom when teachers are watching what you are doing, and we find the schools who really know what they are doing they are not only blocking social networks. They are blocking ESPN, other sites that are not school oriented. Because, during the school day, kids are supposed to be studying.

So there may be easier ways of dealing with it that aren't as hard to craft that won't turn off the entire Internet and will be more effective to the real issue.

To my knowledge, around the country, I have not found a case where a child has been groomed and sexually exploited because of their access from a school computer or a library computer on a social network. I think, instead, if we target getting the FTC involved on a global site that is doing Internet safety, they have got online on guard already, we are partnering with them, getting more stuff into the hands of parents, getting kids aware that even smart kids can be targeted and that whatever you post online is public, and that that cute 14-year-old boy may not be a cute 14-year-old boy, if we can get out there and get everyone involved talking together, we can stop the turf wars, find out what our group does well, find out what NickNick does well. Get the Facebook and the others to put out PSAs, work with the AGs. I think if we pulled together globally--and I think that this committee can help us do that--we can come up with answers. We can make a real difference, and that could be easier.

MR. ENGEL. Thank you.

Let me ask Ms. Yoke, from the ALA point of view, H.R. 5319, as it is currently drafted, would the ALA support it?

MS. YOKE. Well, the goal of DOPA, keeping children safe, is a lot of bull. ALA argues that a more effective and long-term solution would be for Congress to authorize and provide appropriate funding for Internet education programs that would provide resources and support for adequate numbers of qualified school library media specialists and public librarians to serve the young people in our communities by providing information literacy instruction, Internet safety instruction and so on.

ALA suggests that Congress does not need to pass another bill calling for technological measures to control Internet content. Existing CIPA provisions as well as the local policies and activities of our school and public libraries are sufficient. If Congress feels that it must pass such a bill, we would ask that libraries be included in the FCC Advisory Committee, the terminology be clarified and that local decisions be respected.

MR. ENGEL. Thank you.

I would just like to ask, with the Chairman's indulgence, one question. I mentioned the spoofing bill and said we are always playing catch-up. The Internet, obviously, from what everyone is saying, and we know this, is becoming an enabling technology for predators. Are any of you aware or can share with us what other technologies are out there or in research and development that we can use to combat and track down predators? Anyone aware of anything that is out there? Yes.

MS. AFTAB. Social networks can be very helpful in tracking predators. By putting a button on the profiles, the kids can very easily report inappropriate communications with them; and it is a great way of doing it. I know Facebook is very responsive to abuse reports. The YFly site has a "report a creep" button. If someone talks to them, they will report it to law enforcement. It is a great way of mobilizing people and reporting bad things.

In addition, if you can have a central site so that people know where to report different kinds of crimes. The CyberTipLine is fabulous for missing child issues and child pornography issues, but it may not be appropriate for cyber bullying. People need to know where to go when bad things happen to make them stop, and I think that using social networks and other sites like that to let people know where to report them can be very helpful.

MR. KELLY. We have built very extensive reporting tools into our site and background monitoring tools for potentially inappropriate activities on the network that will highlight accounts that could be being misused in terms of too many friend requests, especially too many rejected friend requests, somebody just trying to make the initial connections, and that basically enforces the protections of the user information that we have built into the architecture of our system.

MR. ENGEL. Thank you. Thank you, Mr. Chairman.

MR. FERGUSON. The author of the bill that we are discussing today, the gentleman from Pennsylvania, Mr. Fitzpatrick, is recognized for questions.

MR. FITZPATRICK. Thank you, Mr. Chairman.

First of all, I appreciate all the suggestions of the members of the panel, some very good ones about the need to educate children about the dangers of surfing on the Internet, who is out there lurking beyond where they can see. It is not just educating children, as we have heard from many of the members, educating the parents, Members of Congress, educators. We certainly need to do all that.

And, Mr. Davis, I certainly applaud the steps that Fairfax County Public Schools have taken. As you indicate in your testimony, you have implemented software technology. I think you indicated you may have procedures in place. You are educating children as well.

But the purpose of this hearing in discussing the Deleting Online Predators Act is to talk about the efficacy or would it make sense to protect children unsupervised while in a school computer lab setting from being able to access sites like MySpace.com. We do know from the testimony of the prosecutors who were here that there are cases of predators who are out there and predators who have used the site to get to children, and so we know the predators are on the sites. They are on MySpace, and MySpace is in the school.

You seem to be saying, Mr. Davis, it is okay for MySpace.com to be in the schools as long as we have a policy and we try to monitor it. Wouldn't it be better in the school setting, just in the educational setting, to be prohibiting access to that site because we know that there are predators on that site, a predator we would not--as Mr. Zellis indicated, we would not let a sexual predator walk through the front door of the school, but we are permitting them access to the school and classroom setting through the Internet. What kind of policies can you have in place to protect children from that access?

MR. DAVIS. Okay. I am not saying that it is okay for students to have access to this in schools. In fact, FCPS, we have blocked access to these sites for our students.

What I am getting at is that the benefits of imposing this--for one, school systems that are already subject to or are using E-rate funds are subject to the Children's Internet Protection Act, are addressing this issue. I would expect my colleagues across the country to already be looking at these sites and already making a decision whether that is appropriate for their school to block or not to block that site.

FCPS, we have decided to block that site. I know neighboring jurisdictions have made that decision as well.

So, no, I am not saying that it is okay. My fundamental point is that the benefits would be marginal. Marginal benefits, though, as indicated down here earlier, if it protects one child that is very important. I truly believe that our students have to be prepared to deal with these dangers in life, because that is where they are going to experience it.

There was a comment made earlier about technology and its role in this. Often, technology is accused of having created this problem, and we look to technology to solve this problem. But, in fact, it is people who have created this problem, and it is the people who create these problems that we need to target with legislation.

MR. FITZPATRICK. I guess my next question would be to the prosecutors on the panel. Mr. Abbott, who has taken leave for a moment. He is gone.

Mr. Zellis, I guess this question could be to you. You spend your lifetime prosecuting criminals and you see during the course of your time as a district attorney in Bucks County the methods that predators prey on children has changed now in the age of the Internet. I mean, would that be a safe thing to say, that the use of social networking sites has given predators a new entree to children and is it creating greater challenges for prosecutors such as yourself?

MR. ZELLIS. As I stated before, it has reinvigorated and has given them a new outlet for preying on children. What happens is this is done totally unbeknownst to the parents. As we went around the county, parents are beside themselves when, as the Attorney General said, in Texas--and it was no different in Bucks County--we did live online presentations, and it just took a few minutes to put up on display somebody posing as a teenager--teenage girl in this instance--and there were hits galore; and it frightened and shocked every parent in the town hall meeting.

So we have made adjustments as prosecutors. I know the court system has made adjustments in dealing with it. But we are playing catch-up.

MR. FITZPATRICK. In your opinion, in interviewing child victims as witnesses for cases in Bucks County or perhaps other anecdotal evidence you may have seen, are children prepared for the dangers that they encounter while surfing on the Internet?

MR. ZELLIS. I don't think any child is prepared for it. I think the notion that children have to learn what the real life is like, I don't think any child could be prepared for what they are seeing on the Internet, and these are children who don't even expect it. They are just typing out instant messages to a friend, and all of a sudden somebody pops in there. And it might be pornography, it might be explicit language, or it could just be somebody who is trolling around and trying to groom children.

So, ultimately it is a major, major problem, and you don't expect when you are sending your child to school after monitoring their computer use at home or after sending the child to the library after monitoring their use at home they are going to be exposed to this in the school or library. I certainly wouldn't expect that of my children, and I watch their computer use at home. So to think I would send them to school or to the library, they would have unfettered or easy access to these social networks that they don't have access to at home, I think gets one's blood boiling; and I think for the most part most Americans think that kids don't have easy access to these social networks when they go to school or they go to the library.

MR. FITZPATRICK. It sounds like in Bucks County you have done a number of town hall meetings. You have done Internet safety courses. Is that your experience? Is that what parents are telling you?

MR. ZELLIS. Yes, it is. I think parents want to know more, and that is why I think the FTC part of the legislation is so critical to this legislation. But I also think that parents would be shocked to find out that their kids are going to school and while we are telling the parents you have to monitor them at home and watch what they are doing on the Internet that in school that they have easy access to these sites.

MR. FERGUSON. We are going to go to Mr. Kirk for questions.

MR. KIRK. Thank you, Mr. Chairman; and, once again, thank you for having me on this committee. I applaud this legislation by Congressman Fitzpatrick and this hearing.

The one thing in our panel we have no formal representative of what I would regard as the most important group, parents, and I think the feeling that I hear from them is overwhelming with regard to this legislation. So my guess is, Mr. Zellis, that since you are a prosecutor, you are probably the closest thing to a parental representative here as we can get.

I am encouraged by a different corporate policy by one social networking site and discouraged by another. Facebook is here. And because Facebook's corporate culture--if you can talk about a 2-year-old company having a corporate culture--Facebook's corporate culture is, because it required the dot edu address at the beginning, meant that we were overwhelmingly dealing with adults who had crossed the age of 18. And I think that we should have as free and open access on the Internet as adults as possible, but our law does not say that with regard to children. There is compelling State interest to protect children and their abilities and their rights.

And while Facebook is expanding into the high school arena, that concerns me. Because now you are starting to deal with children. It seems to be very responsive and responsible corporate policy to deny access to anyone who is not in the same school e-mail group. So only a sexual predator who is actually going to school or a teacher can now get access to those kids, but it would be a worry.

MR. KELLY. We are very worried about that.

MR. KIRK. Right, as you should. Because there is a lack of common sense here.

In Highland Park, Illinois, we have spent an awful lot securing the doors of the school. As a Congressman, when I come to school, I have to report to the administrator before I can go anywhere, and I am usually challenged by three or four people walking through the school. And yet MySpace can get an Internet predator into the school library unhindered. That should be an enormous problem.

When we look at the legislation that is currently drafted, I can see that easy access is a definitional point, and I might suggest one that would make me comfortable, that easy access to be defined as any site that has over 100,000 children online. At that point, I really pretty much know who I am talking about. And the hundred grand worth of children is a pretty big group to then begin to think about the United States' legal tradition of forcing anyone who makes money off of children to offer a unique level of protection.

I just think about when we are in the business of making school buses or in selling toys to children, we have unique legal burdens; and if you get in the business of making money off of children, you have a unique legal burden. I mean, this legislation calls for screening.

The other approach, if it was written by the other party from the start and we could go down this road, is just to let trial lawyers rip you to pieces, open up a whole series of Federal liabilities and Federal lawsuits that could be leveled against you and go at it that way.

So I would just say that the Facebook direction is the way to go, except I might hold your business plan at less high school and more the rest.

With regard to privacy rights of kids, we also talk about I think it was one Pennsylvania mom that said, I know that all Americans have rights, but with regard to my children at home, I am their judge, jury, and executioner. And I think that largely reflects the view of a parent.

My question is for David. In your testimony, you just outlined that MySpace.com has now been a center of drug activity, of gang activity, and of Internet predators, that if it was any other business in any other area would be of unique concern to county law enforcement. Isn't it entirely appropriate that the State get involved, especially when we are dealing with children?

MR. ZELLIS. Absolutely. In fact, I brought a picture of a MySpace posting which deals with a gang member; and at the bottom it says, which gang you should be in? And it is the Crips. It is a recruitment tool used in suburban Bucks County or any suburbia around the country. So, these pose new and unique challenges to all of us.

We had in Bucks County one of the first cases involving the sale of drugs to--and it was a minor who--so the whole idea of the age as being the be-all and end-all--this was a juvenile who had a posting with drugs, with guns; and he was in the business of selling drugs on MySpace.

MR. KIRK. We just heard in Levittown, Pennsylvania, of a gang putting a hit out on the class president; and the high school graduation had to be cancelled.

I would just say in Bucks County--I know the answer to this, but in Bucks County is it legal for a gang to come into a library and recruit children?

MR. ZELLIS. No.

MR. KIRK. Right. Nationally, we know from the Drug Enforcement Administration and ATF that the average drug gang shooter is in the seventh grade. So since we have done so much to protect gang recruiting and prevented that from happening in a library or in a school, shouldn't we prevent it from happening in a library or a school via the Internet?

MR. ZELLIS. One would hope.

MR. KIRK. Right. Thank you, Mr. Chairman.

MR. FERGUSON. I want to thank all of our panelists for being here today. This is an extremely important discussion that we are having. It is my hope that we will continue to discuss this topic. We certainly thank our out-of-town guests for coming in and thank Mr. Fitzpatrick and Mr. Kirk for joining us today.

With that, this hearing is adjourned.

[Whereupon, at 1:03 p.m., the subcommittee was adjourned.]

SUBMISSION FOR THE RECORD OF ELIZABETH RACINE

Dear Mr. Chairman:

My name is Elizabeth Racine; I am the mother of three teenagers, and have been a writer, editor, and researcher for the past 21 years, specializing in family and parenting issues. I've appeared in print over 300 times, with articles in *Newsday,* The *Chicago Tribune,* as well as in *Catholic Parent* Magazine, *Today's Catholic Teacher*, and *Momentum* Magazine. I began using the Internet extensively in 1994 for my own research projects as well as for those of my editorial clients. Starting in the year 2000, I taught eighth grade in Catholic schools for four years before returning to full-time freelancing.

As my own children began using the Internet, I have vigorously monitored their online usage, as well as that of my students, with varying degrees of success. Over the past 12 years I have grown increasingly concerned-- and now alarmed-- about not only what is available for viewing online, especially to our children, but also what our children are posting online as well.

For the past few years I have been giving talks to parents, teachers and clergy about these dangers. My real-life stories and images have shocked audiences, who previously had no idea that this problem existed.

I have served as a resource person for many Catholic reporters, and recently appeared on Fox 29's special report on Internet abuses by children. Despite the increasing news coverage, there is still a vast amount of Internet activity that goes unreported.

Lately I have been meeting with members of the House of Representatives and the Senate to educate and advise them on these Internet risks to our children, in hope that they will increase legislation and regulation to help protect them.

I am grateful for Mike Fitzpatrick's Bill, H.R. 5319, the Deleting Online Predators Act of 2006. While it is not foolproof, it is a starting point, a beacon of hope for those, like me, who have seen the Internet's underbelly and are alarmed over what is happening to our children online.

My goal in writing to you today is to help you better understand this attack on our children. It is my great hope that Congress will assist parents, like me, who are intensely concerned about our children's moral and spiritual development. It is time that Congress steps in to help parents protect their children.

I began using the Internet in 1994, and my interest in the Internet changed abruptly when my then-7-year-old son came to me one day while I was in the garage.

"Mommy…" he started, lower lip trembling, "I saw something on the computer…" he looked up helplessly when he couldn't find the words. Worried, I asked him to explain what happened.

"I was playing games on Lego.com and then when I was done, I wanted to find more games for boys to play –so I typed in 'boys.com…'"

And then he stopped. Seeing his agitation, I ran to the computer to see what would possibly be upsetting him (this was 1997, long before public awareness of rampant pornography). I typed in boys.com and was greeted by an image of a young boy, about 12 or 13, performing oral sex on a man. My 9-year-old daughter then piped in that she decided to check girls.com also, and found an equally appalling photo on that site.

Words cannot adequately describe the dark feeling in the pit of my stomach or the primordial mother-bear rage that went through me over this loss of my precious children's innocence. This feeling still wells up in me; my eyes again fill with tears as I write these words. No matter how many times I try, I cannot tell this story without crying, which is embarrassing, even though I have told this story numerous times to parent and teacher groups, trying to get parents to pay attention to what their children are doing online. I endure this willingly in order to protect the children who are being sought so desperately by an industry—indeed, a society-- that is *professing* to try to keep them safe, but is more concerned with "free speech" instead of the protection of children.

Pornographers and its millions of consumers, are only too happy to snare them into the web of addiction to pornography to keep them coming back for more. Parents and teachers need to be made aware of the need to protect our children, at home and at school and the library, so that their innocent web wanderings don't turn into a nightmare.

We moved to our current home in the year 2000, where we enrolled our children in Catholic school. My 12-year-old daughter began using Instant Messenger along with her classmates. I would check to see what was going on—I would use drop-down menus and see what profiles on the kids were posting, and which ones they were viewing. I was in for the shock of my life…one boy had a profile on AOL Hometown, and his profile included graphic porn cartoons and links to porn sites, when all these porn sites started opening rapid-fire on my computer. If you've ever had this happen, you don't soon forget it…a link opens, and then ten, twenty, even thirty windows pop open on your screen, and you can't stop them—and they are all pornographic. I was aghast, and very angry—how can MY computer be subject to this?

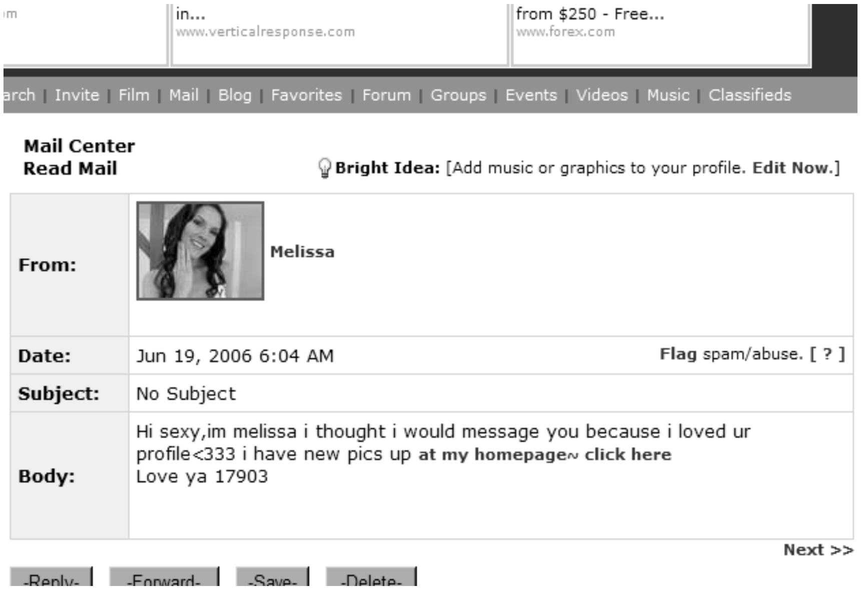
I became a substitute teacher at their school the first year, and was asked to become a teacher the following year. I would be teaching 8th grade—the same grade that my daughter would be enrolled in. She would not be in my class, but her friends would. I still read more and more Internet entries, and came across a saved conversation between my daughter and her "friends." The language and the cyber bullying that went on were atrocious. And here it was, coming from *12-year-olds!!* Their parents had no idea that they were posting this material.

This was in 2001. My school became the recipient of a grant from the Connelly Foundation to receive a laptop cart, enabling the children to have access to a wireless Internet system. Because of my prior research, I knew first-hand the dangers of inappropriate content on the web, and our school had in place a technology person who had a blocking software program installed. We had very strict rules about the kids accessing websites in the classroom, and what to do if something inappropriate came up on the screen—the kids were to close the laptop and raise their hand if the blocking screen came up, or if something appeared that was out of order. As we visited educational websites together as a class, I can't tell you the number of times a child received a red "Blocked" screen, telling me that they had come upon a site with content deemed inappropriate—due to their typing in the educational site's name incorrectly for example—a common ploy of pornographers, who like to purchase the URLs of misspelled site names in hopes of luring in unsuspecting visitors. For example, one of my students tried to access the educational site we were using in class (Funbrain.com), but accidentally transposed two of the letters in its name (FunBrian.com). His computer brought up a red screen, which meant it was blocked.

Also, it is common for pornographers to purchase expired domain names, especially educational websites or those with Catholic or religious titles. This is a hot market--they bank on the fact that people would innocently click on their stored bookmarks and then would be brought to a porn website instead of the religious site they were looking for.

I have researched kids' use of blog sites, now called Social Networking sites, since my own children began using them in 1999. The first ones were the profile sites on Instant Messenger, which could then host "sub-profiles." These sub-profiles allowed children to post all sorts of information about themselves, and I immediately saw the danger in them, since kids could write whatever they wanted on them, and many posted pornography. I tried to alert parents to this danger and met with varying levels of response—some were happy to know so they could correct matters, others said I was out to get their kids and that I was lying about what had been posted! Since I was teaching at the time, this put me in a very awkward position.

With the exponential growth of the latest social networking sites, MySpace being the most popular, I have had my own accounts on all of them, and have been solicited by porn stars – all the big name porn stars try to lure visitors to their own MySpace pages, which feature very suggestive photos, and then, of course, links to the porn site. I have posted one such solicitation below, which leads to a live web-cam site. I received another one today, which invited me to join a MySpace group which is pornographic. I visited the group to see what it was about, and I saw comments posted by lots of kids who were under 18, and who were upset that they had been solicited! So there is hope there, but I can't imagine how many more kids were only too happy to visit the web cam site and participate in the goings-on.


in...
www.verticalresponse.com
from $250 - Free...
www.forex.com
arch | Invite | Film | Mail | Blog | Favorites | Forum | Groups | Events | Videos | Music | Classifieds
Next >>
-Reply-
-Forward-
-Save-
-Delete-

Mail Center
Read Mail

Bright Idea: [Add music or graphics to your profile. **Edit Now.**]

From:	**Melissa**
Date:	Jun 19, 2006 6:04 AM **Flag** spam/abuse. [?]
Subject:	No Subject
Body:	Hi sexy,im melissa i thought i would message you because i loved ur profile<333 i have new pics up **at my homepage~ click here** Love ya 17903

The link in her site leads to the following websites:
www.imlivenow.net and www.ezezdates.info

On the www.imlivenow.net site, there are pictures of Melissa along with this message:

"These pictures are not very revealing because kids may
see this page. On my webcam I get naked and nasty ;]
All you have to do is Click here for your FREE Password

Anyone who has spent any amount of time trolling the pages on MySpace, Xanga, or other social networking sites cannot help but see what a cesspool it is…it's no surprise to me that there is an increasing number of child predator solicitations, leading to rape and even murder. The thing I CANNOT believe is that all schools are not required to have a blocking mechanism in place for the students' safety and well-being. Kids are very interested in these sites and very excited to interact with their friends online—and their hormones are raging and most of them cannot pass up the temptation to view porn. They are oblivious to the danger, even when they are educated.

Even from a schoolwork standpoint, as a teacher, I can't imagine trying to teach and having to compete with kids who might be more interested in clicking over to their MySpace account during a class assignment, and having that eat up their academic learning time. And from what I read on MySpace, they do it ALL THE TIME during class. A teacher cannot visually see every computer at every moment, so it is only too easy for kids to do this.

Libraries are another place that blocking software should be mandatory. Recent news stories show that news crews have filmed men masturbating right there in the open at the library while viewing porn on the library computer—only a few feet away from the children's room. My stomach lurches when I hear of this taking place—how can we not put an end to that sort of thing? What kind of sick society allows that to happen, when the answer is readily available in the form of blocking technology.

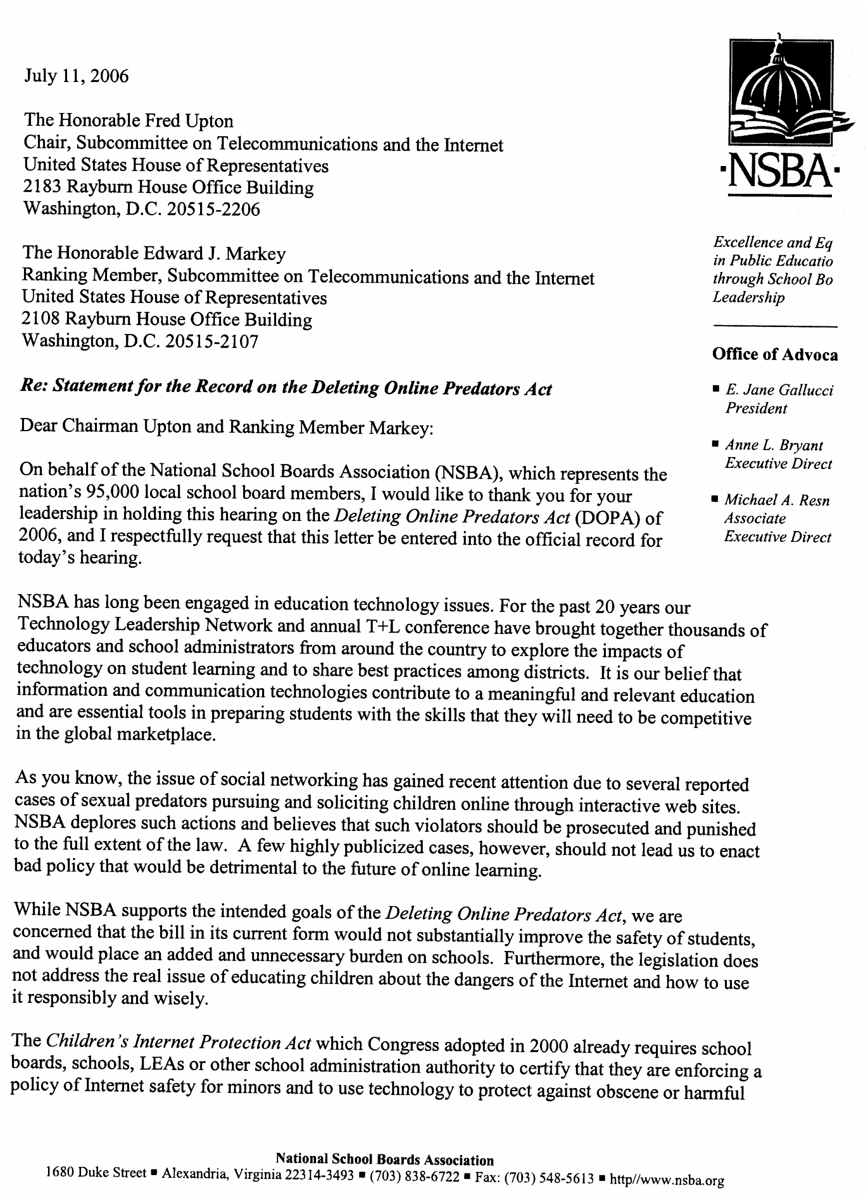
WKYC in Cleveland had an expose on this recently: http://www.wkyc.com/news/news_article.aspx?storyid=52623

> We can't really show you, we have video of Cooper pleasuring himself while watching porn at the Berea Library, just across the room from the children's section.
>
> Take our word for it. And his.
>
> "I wasn't thinking. I made a mistake," Cooper admitted.
>
> If Cooper doesn't trust himself, should we? Well, apparently, the Berea Library does.
>
> Berea Library Manager Cindy Bereznay said she saw Cooper masturbating the last time he was in her library.
>
> Bereznay said they caught Cooper in the act a few years ago.
>
> "I told him I would have to call the police if it continued," she said.
>
> And Cooper ran out of the building.

I realize that H.R. 5319 is not foolproof, because blocking technology is not foolproof. Unfortunately, blocking technology can be circumvented, and there are numerous sites being made available to children to allow them to get around their school or home blocking software—these sites are run by adults, which I can hardly believe. But, just because the mechanism isn't foolproof does not mean we shouldn't implement it. Just as seatbelts are not a guarantee that no harm will come to someone who wears one, so blocking technology is to children. Blocking inappropriate content will protect children more than the alternative, which is to allow everything to come to them unfiltered. It is better to do something rather than to do nothing. In the near future, an organization called CP80 (www.cp80.org) will unveil its simple yet ingenious plan to protect our children while it still allows for free speech.

In the meantime, I implore Congress to evaluate seriously these threats to our children and make their protection their foremost concern. H.R. 5319 is a solid beginning, and I ask that it be implemented, along with other bills that seek to protect our children online.

SUBMISSION FOR THE RECORD OF MICHAEL A RESNICK, ASSOCIATE EXECUTIVE DIRECTOR, NATIONAL SCHOOL BOARDS ASSOCIATION



·NSBA·

Excellence and Eq
in Public Educatio
through School Bo
Leadership

Office of Advoca

- *E. Jane Gallucci*
  President
- *Anne L. Bryant*
  Executive Direct
- *Michael A. Resn*
  Associate
  Executive Direct

July 11, 2006

The Honorable Fred Upton
Chair, Subcommittee on Telecommunications and the Internet
United States House of Representatives
2183 Rayburn House Office Building
Washington, D.C. 20515-2206

The Honorable Edward J. Markey
Ranking Member, Subcommittee on Telecommunications and the Internet
United States House of Representatives
2108 Rayburn House Office Building
Washington, D.C. 20515-2107

Re: Statement for the Record on the Deleting Online Predators Act

Dear Chairman Upton and Ranking Member Markey:

On behalf of the National School Boards Association (NSBA), which represents the nation's 95,000 local school board members, I would like to thank you for your leadership in holding this hearing on the *Deleting Online Predators Act* (DOPA) of 2006, and I respectfully request that this letter be entered into the official record for today's hearing.

NSBA has long been engaged in education technology issues. For the past 20 years our Technology Leadership Network and annual T+L conference have brought together thousands of educators and school administrators from around the country to explore the impacts of technology on student learning and to share best practices among districts. It is our belief that information and communication technologies contribute to a meaningful and relevant education and are essential tools in preparing students with the skills that they will need to be competitive in the global marketplace.

As you know, the issue of social networking has gained recent attention due to several reported cases of sexual predators pursuing and soliciting children online through interactive web sites. NSBA deplores such actions and believes that such violators should be prosecuted and punished to the full extent of the law. A few highly publicized cases, however, should not lead us to enact bad policy that would be detrimental to the future of online learning.

While NSBA supports the intended goals of the *Deleting Online Predators Act*, we are concerned that the bill in its current form would not substantially improve the safety of students, and would place an added and unnecessary burden on schools. Furthermore, the legislation does not address the real issue of educating children about the dangers of the Internet and how to use it responsibly and wisely.

The *Children's Internet Protection Act* which Congress adopted in 2000 already requires school boards, schools, LEAs or other school administration authority to certify that they are enforcing a policy of Internet safety for minors and to use technology to protect against obscene or harmful material. As a result, school districts have the power to block access to social networking sites and chat rooms, and a number of them have chosen to do so. A federal mandate requiring school districts to block all social networking sites, however, would impose additional restrictions on schools and usurp the authority of local school districts to determine what content should flow into schools. In addition, the requirement would impose a greater burden on E-rate applicants, which could deter some schools from participating in the Internet access program.

The proposed ban on social networking sites could also eliminate some very innovate practices in schools such as teacher use of blogs. For example, one educator in Liberty, MO uses a blog and podcast for American history lessons and has had downloads from around the world. Another teacher in Orange City schools in Ohio, uses a blog for 4th graders to become "book critics" by posting their book reports online. While DOPA allows for the disabling of blockage software by adults or minors with adult supervision for <u>educational</u> purposes, this process is unrealistic and would be cumbersome and difficult to enforce. Unlike current restrictions against obscene materials that can be objectively identified, this legislation would require schools to subjectively predict which sites may be misused. Identifying and evaluating such sites are not compatible with the technical capabilities of filtering vendors and are likely to lead to blocking of legitimate instructional sites.

Furthermore, the blockage of social networking sites while children are at school does not adequately prepare them to deal with the potential dangers of online predators outside of school and how to deal responsibly on the Internet. These software filters and other blockage devises provide a false sense of security for America's children. Whether students are able to access these sites at school or not, they still need to know the right way to navigate and conduct themselves in a Web 2.0 environment where they are now the creators of web-based content.

According to recent data, 87% of students 12-17 are online and 65 million young people have accessed social networking sites. Given this reality, we cannot afford to "duck" our responsibility to educate our children by hiding behind filters to block these sites. Education is the key to preparing our students to interact safely on the Internet. Together, the education community, parents, and others can help to instill responsible decision-making and empower students to recognize the lures of online predators.

On behalf of school board members across the country, NSBA thanks you for your attention to this important issue. We look forward to working with you to ensure that America's schoolchildren receive and safe and valuable educational experience.

Sincerely,

A

Michael A. Resnick
Associate Executive Director

MAR:cg/mh
N:Adv/LtrDOPAHearing.7.11.06