

# PROTECTING YOUTHS IN AN ONLINE WORLD

---

---

## HEARING

BEFORE THE

SUBCOMMITTEE ON CONSUMER PROTECTION,  
PRODUCT SAFETY, AND INSURANCE

OF THE

COMMITTEE ON COMMERCE,  
SCIENCE, AND TRANSPORTATION  
UNITED STATES SENATE

ONE HUNDRED ELEVENTH CONGRESS

SECOND SESSION

—————  
JULY 15, 2010  
—————

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



U.S. GOVERNMENT PRINTING OFFICE

67-765 PDF

WASHINGTON : 2011

---

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

SENATE COMMITTEE ON COMMERCE, SCIENCE, AND TRANSPORTATION

ONE HUNDRED ELEVENTH CONGRESS

SECOND SESSION

JOHN D. ROCKEFELLER IV, West Virginia, *Chairman*

DANIEL K. INOUE, Hawaii	KAY BAILEY HUTCHISON, Texas, <i>Ranking</i>
JOHN F. KERRY, Massachusetts	OLYMPIA J. SNOWE, Maine
BYRON L. DORGAN, North Dakota	JOHN ENSIGN, Nevada
BARBARA BOXER, California	JIM DEMINT, South Carolina
BILL NELSON, Florida	JOHN THUNE, South Dakota
MARIA CANTWELL, Washington	ROGER F. WICKER, Mississippi
FRANK R. LAUTENBERG, New Jersey	GEORGE S. LEMIEUX, Florida
MARK PRYOR, Arkansas	JOHNNY ISAKSON, Georgia
CLAIRE McCASKILL, Missouri	DAVID VITTER, Louisiana
AMY KLOBUCHAR, Minnesota	SAM BROWNBACK, Kansas
TOM UDALL, New Mexico	MIKE JOHANNIS, Nebraska
MARK WARNER, Virginia	
MARK BEGICH, Alaska	

ELLEN L. DONESKI, *Staff Director*

JAMES REID, *Deputy Staff Director*

BRUCE H. ANDREWS, *General Counsel*

ANN BEGEMAN, *Republican Staff Director*

BRIAN M. HENDRICKS, *Republican General Counsel*

NICK ROSSI, *Republican Chief Counsel*

---

SUBCOMMITTEE ON CONSUMER PROTECTION, PRODUCT SAFETY, AND  
INSURANCE

MARK PRYOR, Arkansas, <i>Chairman</i>	ROGER F. WICKER, Mississippi, <i>Ranking</i>
BYRON L. DORGAN, North Dakota	OLYMPIA J. SNOWE, Maine
BARBARA BOXER, California	JIM DEMINT, South Carolina
BILL NELSON, Florida	JOHN THUNE, South Dakota
CLAIRE McCASKILL, Missouri	JOHNNY ISAKSON, Georgia
AMY KLOBUCHAR, Minnesota	DAVID VITTER, Louisiana
TOM UDALL, New Mexico	

## CONTENTS

	Page
Hearing held on July 15, 2010 .....	1
Statement of Senator Pryor .....	1
Statement of Senator Rockefeller .....	31
Prepared statement .....	31
Statement of Senator Wicker .....	34
Prepared statement .....	34
Statement of Senator Klobuchar .....	37

### WITNESSES

Jessica Rich, Deputy Director, Bureau of Consumer Protection, Federal Trade Commission .....	3
Prepared statement .....	5
Hemanshu Nigam, Co-Chair, Online Safety Technology Working Group; Safety Advisor, News Corporation; and Founder, SSP Blue .....	11
Prepared statement .....	13
Jeff McIntyre, Director—National Policy, Children Now .....	16
Prepared statement .....	18
Michelle Collins, Vice President, Exploited Children Division, The National Center for Missing & Exploited Children .....	19
Prepared statement .....	21
K. Dane Snowden, Vice President, External and State Affairs, CTIA—the Wireless Association® .....	23
Prepared statement .....	25

### APPENDIX

Letter, dated July 15, 2010 to Chairman Mark Pryor and Ranking Member Roger Wicker, Subcommittee on Consumer Protection, Product Safety, and Insurance, U.S. Senate from Laura W. Murphy, Director, Washington Legislative Office and Michael W. Macleod-Ball, Chief Legislative and Policy Counsel, American Civil Liberties Union .....	57
Yahoo!, Inc., prepared statement .....	59



# PROTECTING YOUTHS IN AN ONLINE WORLD

---

THURSDAY, JULY 15, 2010

U.S. SENATE,  
SUBCOMMITTEE ON CONSUMER PROTECTION, PRODUCT  
SAFETY, AND INSURANCE,  
COMMITTEE ON COMMERCE, SCIENCE, AND TRANSPORTATION,  
*Washington, DC.*

The Subcommittee met, pursuant to notice, at 2:02 p.m. in room SR-253, Russell Senate Office Building, Hon. Mark Pryor, Chairman of the Subcommittee, presiding.

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

Senator PRYOR. I'll go ahead and call this hearing to order.

And I want to thank all of our witnesses and our audience members for being here.

We are, if you all have probably noticed, we're kind of scurrying around here to figure out the schedule. As is the custom in the U.S. Senate, the schedule is changing rapidly, and we now have a roll-call vote that has just started on the floor. And, even though I think we're going to have several members participate today, the rollcall vote is going to, you know, upset the smooth flow of this hearing.

But, nonetheless, what I thought I would do is give a brief opening statement, and if Senator Wicker's able to make it here before the vote, let him give his statement. And if he's not able or no one else is able to be here, go ahead and try to get as far along as we can before I have to recess and go vote. And if I have a fellow subcommittee member here, we'll just continue the hearing, but we may have to recess in order to get these two votes behind us. But, anyway, that's just housekeeping.

Thank you all for being here. And I really appreciate the time and effort that you have made to be here for our hearing on protecting youths in an online world.

As I said, the Subcommittee members may be coming and going and a little bit disrupted because of the vote on the floor. But, this is a follow-up hearing to the children's privacy hearing we held in April, and the second in a series to consider how to best protect our young people online.

Young people are spending an increasing amount of time on the Internet. They have Internet access points in their cell phones through which they can now connect to social networking sites, play games, and use various apps. According to one reporter, approximately 83 percent of 17-year-olds and over 50 percent of 12-

year-olds now own a cell phone. Despite the valuable benefits of technology—and those are many—some young people can be hurt by this instant access.

Researchers are seeing disturbing trends in cyberbullying and harassment, among other risky online behaviors, including the forwarding or sending of sexually explicit messages. According to one Cox Communications Teen Online Safety and Digital Reputation Survey, approximately one-third of teenagers using the Internet report they have been victims of online harassment. Recent press articles have highlighted injurious practices among teens who tease and harass their peers online, creating hurt feelings and uncomfortable learning environments.

A recent *New York Times* article, entitled “Online Bullies Pull Schools Into the Fray,” underscored the pain that some middle school students are facing when targeted by, or bullied by, their peers online. The article captured the complexity surrounding this debate, how to teach expectations of behavior while promoting parental control and discipline, empowering educators, strengthening school safety, and protecting privacy concerns.

A few years ago, one press article featured a student from Fayetteville, Arkansas, who experienced aggressive bullying both online and offline. In junior high, the student was hit so hard he lost consciousness. In 9th grade he was struck with so much force that his braces became caught on the inside of his cheek. Some of his classmates started a page on Facebook called “Everyone that hates” and then inserted the name of the child.

When I hear about the psychological and emotional damage inflicted on teenagers and younger children as a result of cyberbullying, online harassment, or forms of exploitation online, I become deeply concerned, both as a father and as a lawmaker. Children deserve to learn in peace and safety. I believe that is one basic premise upon which we all should be able to agree.

I look forward to hearing from the Federal Trade Commission about how its education campaign for online socializing is working, whether improvements can be made, and how we can create solutions together to strengthen the online safety and security of our Nation’s children.

I also look forward to hearing from the witnesses about the greatest threats to minors’ safety in the online space, strategies to mitigate them, suggestions for promoting safe use of digital media, and how the FTC could work with other groups or schools to encourage safe navigation of online sites to better defend against risks to their mental health and well-being.

It is critical that we work together to determine how to integrate the research of our online media and technology experts, our public, private, and law enforcement officials, and agencies’ staff the—at the Federal Trade Commission to craft meaningful and effective policies to better protect our young people against threats on the Internet.

So, what I’d like to do now is go ahead and introduce our panels here and get as far along as possible with their opening statements. And again, I may have to recess at some point during the—you know, during the middle of the panel opening statements.

But, I'll go ahead and just very briefly say—let's see, in order we have, Ms. Jessica Rich, Deputy Director of Bureau of Consumer Protection, Federal Trade Commission; Mr. Hemanshu Nigam, Safety Advisor, News Corporation, and Founder of SSP Blue, and former Chief Safety and Security Officer for MySpace; Mr. Jeff McIntyre, Director of National Policy for Children Now; Ms. Michelle Collins, Vice President, Exploited Children Division, National Center for Missing & Exploited Children; and Mr. K. Dane Snowden, Vice President, External and State Affairs, CTIA—The Wireless Association.

Ms. Rich, would you mind leading us off?

**STATEMENT OF JESSICA RICH, DEPUTY DIRECTOR, BUREAU OF CONSUMER PROTECTION, FEDERAL TRADE COMMISSION**

Ms. RICH. Chairman Pryor, my name is Jessica Rich, Deputy Director of the Bureau of Consumer Protection with the Federal Trade Commission.

And there I am. I'm on.

[Laughter.]

Ms. RICH. I appreciate this opportunity to discuss the Commission's efforts to protect the privacy and security of teens in the digital environment. While the views expressed in this written testimony represent the views of the Commission, my oral testimony and responses to questions are my own, and do not necessarily reflect the views of the Commission or any commissioner.

The Federal Trade Commission is committed to protecting teens as they use and explore the online world. Today, I'll talk about the FTC's efforts to educate teens and parents about cybersafety, enforce the privacy laws, and develop policy approaches to make the digital world safer for all consumers, including teens.

Parents of teens won't be surprised to learn that more teens go online than any other age group, over 90 percent. Teens have earned the nickname "digital natives," since they use the Internet so much to socialize with their peers, learn about topics that interest them, and express themselves. Teens avidly communicate using instant message and social networks, share music and photos on P2P networks, and use smart phones to text, watch videos, and surf the web.

Despite the many positives, teens may be less able to handle some challenges online than adults. For example, teens may not always think about the consequences of their actions, so they may post personal details online without thinking that it could leave them vulnerable to identity theft or cost them a job if a future employer sees it. And problems, once limited to the school hallway or the bus stop, like bullying and harassment, now spill into the online world.

So, what's the FTC doing? First, we educate teens and parents about online threats and how to avoid them. The Commission's online safety portal, *onguardonline.gov*, helps consumers of all ages use the Internet safely and responsibly. Our new booklet, titled "Net Cetera: Chatting With Kids About Being Online," provides practical tips on how parents, teachers, and other trusted adults can talk to kids about issues like cyberbullying, sexting, social networking, mobile phone use, and online privacy. We've already dis-

tributed more than 3.7 million copies of Net Cetera with partners, including school districts and individual schools, and we are actively working to expand the reach of these efforts.

Second, the Commission aggressively enforces existing laws to protect consumers' privacy. Let me highlight just a couple of areas affecting teens: social networks and peer-to-peer file sharing.

About three in four American teens now use social networking sites, nearly half on a daily basis. Since social networking exploded on the youth scene, the Commission has brought a number of enforcement actions against these sites. For example, just 2 weeks ago the Commission announced a consent order against Twitter, settling charges that it falsely represented that it maintain reasonable security and would take reasonable steps to ensure that private tweets remain private.

In addition, many teens use P2P file sharing to share music, games, and software online. P2P programs present privacy and security risks because people may inadvertently allow others to copy private files they never intended to share. The Commission recently sent letters notifying several dozen entities that their customer information had been exposed on P2P file-sharing networks. We also sent them educational materials to help them secure their confidential data and opened nonpublic investigations into the most serious cases.

Third, we're exploring policy approaches that would help all consumers preserve their privacy in commercial settings, including teens. For example, we've been gathering information about social networking as part of a recently concluded series of public roundtables examining ways to foster privacy protections in the Information Age. Participants discussed the difficulty of defining consumer expectations on social working—networking sites, as well as issues related to data collection by numerous third-party applications operating at those sites.

Mobile space is another key area. As the Chairman mentioned, a recent study found that 58 percent of 12-year-olds and 83 percent of 17-year-olds own a cell phone. And an increasing number of teens own more sophisticated smart phones. These devices collect and store information from teens, and host all sorts of third-party applications which do the same. The increasing use of smart phones and similar devices was one of the main reasons we decided to accelerate our review of the Children's Online Privacy Protection Act.

Before I conclude, let me address the scope of COPPA. As you know, some have suggested that COPPA should be extended to teens. COPPA requires websites and online services to obtain parental consent prior to the collection, use, or disclosure of personal information from children. When drafting COPPA, Congress decided to define "child" as under age 13, largely on the basis that most young children don't possess adequate knowledge or judgment to decide if and when to divulge personal information online.

This reasoning does not necessarily extend to adolescents, who have greater access to the Internet outside the home than younger children. Teens may also be less likely than young children to provide their true age or their parents' contact information. And as children approach adulthood and use general-audience websites, it

becomes more difficult to craft laws that don't unduly restrict free speech.

That being said, we are very happy to work with the Committee if it determines to enact legislation providing special protections for teens online. We'll also continue our efforts to educate teens and their parents and develop policy recommendations to protect all consumers, including teens.

In conclusion, the Commission is committed to protecting all consumers in the digital environment, especially those, such as teens, who are particularly vulnerable to threats on the Internet.

Thank you. I look forward to your questions.  
[The prepared statement of Ms. Rich follows:]

PREPARED STATEMENT OF JESSICA RICH, DEPUTY DIRECTOR,  
BUREAU OF CONSUMER PROTECTION, FEDERAL TRADE COMMISSION

## I. Introduction

Chairman Pryor, Ranking Member Wicker, and members of the Subcommittee, my name is Jessica Rich and I am the Deputy Director of the Bureau of Consumer Protection at the Federal Trade Commission ("FTC" or "Commission").<sup>1</sup> I appreciate this opportunity to appear before you today to discuss the Commission's efforts to protect the privacy and security of teens in the digital environment.

The Federal Trade Commission is committed to protecting teens as they navigate digital technologies and applications. The agency has actively engaged in education, law enforcement, and policy efforts to help make the digital world safer for all consumers, including teens.

This testimony first highlights some of the privacy and safety risks teens face as they participate in the digital world. Second, it summarizes the Commission's efforts to educate teens and their parents about these risks. Third, it highlights the Commission's efforts to protect privacy in the context of technologies used heavily by teens in particular—social networking, mobile computing, and peer-to-peer ("P2P") file-sharing programs. Finally, the testimony addresses proposals to create separate privacy protections for teens online.

## II. Teens in the Digital Environment

Teens are heavy users of digital technology and new media applications including social networking, mobile devices, instant messaging, and file-sharing. Indeed, a 2007 study found that over 90 percent of kids between the ages of 12 and 17 spend time online.<sup>2</sup> The online world has changed how teens learn, socialize, and are entertained. In many ways, the experiences teens have online are positive—they use the Internet to socialize with their peers,<sup>3</sup> to learn more about topics that interest them,<sup>4</sup> and to express themselves.<sup>5</sup>

But teens also face unique challenges online. For example, research shows that teens tend to be more impulsive than adults and that they may not think as clearly as adults about the consequences of what they do.<sup>6</sup> As a result, they may voluntarily disclose more information online than they should. On social networking sites, young people may share personal details that leave them vulnerable to identity

<sup>1</sup> While the views expressed in this statement represent the views of the Commission, my oral presentation and responses to questions are my own and do not necessarily reflect the views of the Commission or any individual Commissioner.

<sup>2</sup> Amanda Lenhart, Mary Madden, Alexandra Rankin Macgill, & Aaron Smith, Pew Internet & American Life Project, *Teens and Social Media* (Dec. 19, 2007), available at [www.pewinternet.org/-/media/Files/Reports/2007/PIP\\_Teens\\_Social\\_Media\\_Final.pdf.pdf](http://www.pewinternet.org/-/media/Files/Reports/2007/PIP_Teens_Social_Media_Final.pdf.pdf).

<sup>3</sup> See Amanda Lenhart & Mary Madden, Pew Internet & American Life Project, *Social Networking Websites and Teens* (Jan. 2007), available at [www.pewinternet.org/Reports/2007/Social-Networking-Websites-and-Teens/Data-Memo/Moredetails-from-the-survey.aspx?r=1](http://www.pewinternet.org/Reports/2007/Social-Networking-Websites-and-Teens/Data-Memo/Moredetails-from-the-survey.aspx?r=1).

<sup>4</sup> See Kaiser Family Foundation, *Generation M2: Media in the Lives of 8- to 18-Year-Olds* (Jan. 2010), available at [www.kff.org/entmedia/upload/8010.pdf](http://www.kff.org/entmedia/upload/8010.pdf).

<sup>5</sup> See Amanda Lenhart, Kristen Purcell, Aaron Smith, & Kathryn Zickuhr, Pew Internet & American Life Project, *Social Media and Young Adults* (Feb. 2010), available at [www.pewinternet.org/Reports/2010/Social-Media-and-Young-Adults.aspx?r=1](http://www.pewinternet.org/Reports/2010/Social-Media-and-Young-Adults.aspx?r=1).

<sup>6</sup> See, e.g., Transcript of Exploring Privacy, A Roundtable Series (Mar. 17, 2010), Panel 3: Addressing Sensitive Information, available at [htc-01.media.globix.net/COMP008760MOD1/fic\\_web/transcripts/031710\\_sess3.pdf](http://htc-01.media.globix.net/COMP008760MOD1/fic_web/transcripts/031710_sess3.pdf); Chris Hoofnagle, Jennifer King, Su Li, and Joseph Turov, *How Different Are Young Adults from Older Adults When It Comes to Information Privacy Attitudes & Policies?* (April 14, 2010), available at [ssrn.com/abstract=1589864](http://ssrn.com/abstract=1589864).

theft.<sup>7</sup> They may also share details that could adversely affect their potential employment or college admissions.<sup>8</sup> Teens also sometimes “sex” to their peers—send text messages and images with sexual content—without considering the potential legal consequences and harm to their reputations. According to one recent study, 4 percent of cell phone owners aged 12 to 17 have sent sexually suggestive images of themselves by phone, while 15 percent have received “sexts” containing images of someone they know.<sup>9</sup> In addition, bullies or predators—most often teens’ own peers—may try to take advantage of adolescents on the Internet. About one-third of all teens online have reported experiencing some kind of online harassment, including cyberbullying.<sup>10</sup>

Despite teens’ sharing and use of personal information in the digital world, there is data that suggests teens are concerned about their online privacy. For example, one study of teens and privacy found that teens engage in a variety of techniques to obscure or conceal their real location or personal details on social networking sites.<sup>11</sup> The Commission seeks to address these privacy concerns—as well as parents’ concerns about their teens’ online behavior and interactions—through education, policy development, and law enforcement, as discussed further below.

### III. Consumer Education

The FTC has launched a number of education initiatives designed to encourage consumers of all ages to use the Internet safely and responsibly. The Commission’s online safety portal, OnGuardOnline.gov, developed in partnership with other Federal agencies, provides practical information in a variety of formats—including articles, game, quizzes, and videos—to help people guard against Internet fraud, secure their computers, and protect their personal information.<sup>12</sup> The Commission’s booklet, *Net Cetera: Chatting With Kids About Being Online*,<sup>13</sup> is the most recent addition to the OnGuardOnline.gov consumer education campaign. This guide provides practical tips on how parents, teachers, and other trusted adults can help children of all ages, including teens and pre-teens, reduce the risks of inappropriate conduct, contact, and content that come with living life online.

*Net Cetera* focuses on the importance of communicating with children about issues ranging from cyberbullying to sexting, social networking, mobile phone use, and online privacy. It provides specific advice to parents about talking to their children about each of these topics. For example, on the subject of sexting, it discusses the risks sexting poses to kids’ reputations and friendships—as well as possible legal consequences if kids create, forward, or save these kinds of messages—and gives parents straightforward advice: “Tell your kids not to do it.” With respect to cyberbullying, *Net Cetera* advises parents to talk with their kids about online behavior and about any messages or images that make them feel threatened or hurt. The guide advises parents to work with a child who is being bullied by helping them to not react, save the evidence, and block or delete the bully.

The Commission has partnered with schools, community groups, and local law enforcement to publicize *Net Cetera*, and the agency has distributed more than 3.7 million copies of the guide since it was introduced in October 2009. The FTC will continue to work with other Federal agencies, state departments of education, school districts, and individual schools to distribute *Net Cetera* and *OnGuardOnline.gov* to parents and educators. Additionally, the FTC plans to reach out to other groups that

<sup>7</sup> See Javelin Strategy and Research, 2010 *Identity Fraud Survey Report* (Feb. 2010), available at [www.javelinstrategy.com/uploads/files/1004.R\\_2010IdentityFraudSurveyConsumer.pdf](http://www.javelinstrategy.com/uploads/files/1004.R_2010IdentityFraudSurveyConsumer.pdf).

<sup>8</sup> See e.g., Commonsense Media, *Is Social Networking Changing Childhood? A National Poll* (Aug. 10, 2009), available at [www.common sense media.org/sites/default/files/CSM\\_teen\\_social\\_media\\_080609\\_FINAL.pdf](http://www.common sense media.org/sites/default/files/CSM_teen_social_media_080609_FINAL.pdf) (indicating that 28 percent of teens have shared personal information online that they would not normally share publicly).

<sup>9</sup> Press Release, Pew Internet & American Life Project, *Teens and Sexting* (Dec. 15, 2009), available at [www.pewinternet.org/Press-Releases/2009/Teens-and-Sexting.aspx](http://www.pewinternet.org/Press-Releases/2009/Teens-and-Sexting.aspx).

<sup>10</sup> Amanda Lenhart, Pew Internet & American Life Project, *Cyberbullying and Online Teens* (June 27, 2007), available at [www.pewinternet.org/-/media/Files/Reports/2007/PIP%20Cyberbullying%20Memo.pdf.pdf](http://www.pewinternet.org/-/media/Files/Reports/2007/PIP%20Cyberbullying%20Memo.pdf.pdf).

<sup>11</sup> Amanda Lenhart and Mary Madden, Pew Internet & American Life Project, *Teens, Privacy, and Online Social Networks* (Apr. 18, 2007), available at [www.pewinternet.org/Reports/2007/Teens-Privacy-and-Online-Social-Networks.aspx?r=1](http://www.pewinternet.org/Reports/2007/Teens-Privacy-and-Online-Social-Networks.aspx?r=1).

<sup>12</sup> The *OnGuardOnline.gov* website is the central component of the OnGuardOnline consumer education campaign, a partnership of the Federal Government and the technology community. Currently, 13 Federal agencies and a large number of safety organizations are partners on the website, contributing content and helping to promote and disseminate consistent messages. Since the launch of *OnGuardOnline.gov* and its Spanish-language counterpart *AlertaenLinea.gov* in September 2005, more than 12 million visitors have used these sites for information about computer security.

<sup>13</sup> *Net Cetera* is available online at [www.onguardonline.gov/pdf/tec04.pdf](http://www.onguardonline.gov/pdf/tec04.pdf).

work with kids, such as summer camps, state education technology associations, and scouting organizations to publicize these materials.

In furtherance of the FTC's education efforts, Commission staff also participated in the Online Safety and Technology Working Group (OSTWG), a working group composed of private sector members and Federal agencies. OSTWG reported its findings about youth safety on the Internet to Congress on June 4, 2010.<sup>14</sup> Among its tasks, OSTWG reviewed and evaluated the status of industry efforts to promote online safety through educational efforts, parental control technology, blocking and filtering software, and age-appropriate labels for content. With respect to Internet safety education, OSTWG recommended greater interagency cooperation, publicity, and public-private sector cooperation for projects such as *OnGuardOnline* and *Net Cetera* to improve their national uptake in schools and local communities. As described above, the FTC is actively working to expand the reach of the already successful *OnGuardOnline* and *Net Cetera* projects.

#### IV. Social Networking, Mobile Computing, and P2P

In addition to education efforts to improve teen privacy, the Commission is also focused on specific technologies of which teens are particularly high users—social networking, mobile computing, and P2P file-sharing.

##### A. Social Networking

Social networking is pervasive among teens: 73 percent of American teens aged 12 to 17 now use social networking sites such as Facebook and MySpace, up from 55 percent 2 years ago.<sup>15</sup> Nearly half of teens use these sites on a daily basis to interact with their friends.<sup>16</sup> Teens use social networking to send messages to friends, post comments, and share photos and videos.<sup>17</sup>

The Commission has sought to protect teenage and other consumers in this environment through law enforcement, research, and education. It has brought a number of enforcement actions against social networking sites since 2006, when social networking exploded on the youth scene. Most recently, the Commission announced a consent order against Twitter, Inc. settling charges that it falsely represented to consumers that it would maintain reasonable security of its system and that it would take reasonable steps to ensure that private tweets remain private. Under the order, Twitter has agreed to maintain reasonable security and to obtain independent audits of its security procedures every 2 years for 10 years.<sup>18</sup> The Commission also has brought actions against several social networking sites that targeted youth but failed to adhere to the Children's Online Privacy Protection Act ("COPPA") with respect to users under the age of 13.<sup>19</sup> The Commission will continue to examine the practices of social networking sites and bring enforcement actions when appropriate.

In addition to its enforcement work, the Commission has been gathering information about social networking as part of a recently-concluded series of public roundtables on consumer privacy.<sup>20</sup> The goal of the roundtables was to explore how best to protect consumer privacy without curtailing technological innovation and beneficial uses of information.<sup>21</sup> Participants at the roundtables repeatedly raised

<sup>14</sup> *Youth Safety on a Living Internet: Report of the Online Safety and Technology Working Group* (June 4, 2010), available at [www.ntia.doc.gov/reports/2010/OSTWG\\_Final\\_Report\\_060410.pdf](http://www.ntia.doc.gov/reports/2010/OSTWG_Final_Report_060410.pdf).

<sup>15</sup> See Amanda Lenhart, Kristen Purcell, Aaron Smith, & Kathryn Zickuhr, Pew Internet & American Life Project, *Social Media and Young Adults* (Feb. 2010), available at [www.pewinternet.org/Reports/2010/Social-Media-and-Young-Adults.aspx?r=1](http://www.pewinternet.org/Reports/2010/Social-Media-and-Young-Adults.aspx?r=1).

<sup>16</sup> See Amanda Lenhart & Mary Madden, Pew Internet & American Life Project, *Social Networking Websites and Teens* (Jan. 2007), available at [www.pewinternet.org/Reports/2007/Social-Networking-Websites-and-Teens/Data-Memo/Moredetails-from-the-survey.aspx?r=1.52](http://www.pewinternet.org/Reports/2007/Social-Networking-Websites-and-Teens/Data-Memo/Moredetails-from-the-survey.aspx?r=1.52).

<sup>17</sup> See Amanda Lenhart, Mary Madden, Alexandra Rankin Macgill, & Aaron Smith, Pew Internet & American Life Project, *Teens and Social Media* (Dec. 19, 2007), available at [www.pewinternet.org/-/media/Files/Reports/2007/PIP\\_Teens\\_Social\\_Media\\_Final.pdf.pdf](http://www.pewinternet.org/-/media/Files/Reports/2007/PIP_Teens_Social_Media_Final.pdf.pdf).

<sup>18</sup> *In re Twitter*, FTC File No. 092 3093 (June 24, 2010) (approved for public comment), available at [www.ftc.gov/opa/2010/06/twitter.shtm](http://www.ftc.gov/opa/2010/06/twitter.shtm).

<sup>19</sup> *United States v. Xanga.com, Inc.*, No. 06-CIV-6853(SHS) (S.D.N.Y.) (final order Sept. 11, 2006); *United States v. Industrious Kid, Inc.*, No. 08-CV-0639 (N.D. Cal.) (final order Mar. 6, 2008); *United States v. Sony BMG Music Entm't*, No. 08-CV-10730 (S.D.N.Y.) (final order Dec. 15, 2008); *United States v. Iconix Brand Group, Inc.*, No. 09-CV-8864 (S.D.N.Y.) (final order Nov. 5, 2009).

<sup>20</sup> More information about the Privacy Roundtables can be found at [www.ftc.gov/bcp/workshops/privacyroundtables/index.shtml](http://www.ftc.gov/bcp/workshops/privacyroundtables/index.shtml).

<sup>21</sup> Several key concepts emerged from the roundtable discussions. First, participants stated that data collection and use practices should be more transparent by, for example, simplifying privacy disclosures so that consumers can compare them. Second, participants said that it

issues related to social networking, and a specific panel was devoted to the subject. Experts on this panel discussed the difficulty of defining consumer expectations on social networking sites, issues related to third-party applications that use data from social networking sites, and the effectiveness of privacy disclosures and privacy settings in the social networking space.

The Commission is reviewing the information it received as part of the roundtable series and drafting initial privacy proposals, which it will release for public comment later this year.<sup>22</sup> The Commission will consider the information it obtained about social networking as it makes its recommendations.

### *B. Mobile Technology*

Teens' use of mobile devices is increasing rapidly—in 2004, 45 percent of teens aged 12 to 17 had a cell phone; by 2009, that figure jumped to 75 percent.<sup>23</sup> Many teens are using their phones not just for calling or texting, but increasingly for applications like e-mailing and web browsing, including accessing social networking sites and making online purchases.<sup>24</sup> They are also using relatively new mobile applications that raise unique privacy concerns, such as location-based tracking.<sup>25</sup>

The FTC has been actively addressing privacy issues relating to mobile technology for several years. In 2008, the Commission held a Town Hall meeting to explore the evolving mobile marketplace and its implications for consumer protection policy. Participants in the meeting examined topics such as consumers' ability to control mobile applications and mobile commerce practices targeting children and teens. In April 2009, FTC staff issued a report setting out key findings and recommendations based on the Town Hall meeting. Having highlighted that the increasing use of smartphones presents unique privacy challenges regarding children, the Town Hall meeting led to an expedited regulatory review of the Children's Online Privacy Protection Rule.<sup>26</sup> The review is taking place this year, even though it was originally set for 2015.

More recently, the privacy roundtable discussions devoted a panel to addressing the privacy implications of mobile computing. This panel focused on two significant issues: the extent to which location-based services were proliferating in an environment without any basic rules or standards, and the degree to which transparency of information sharing practices is possible on mobile devices. As with social networking, the Commission staff's upcoming report on the privacy roundtables will further address these issues.

In addition to these policy initiatives, the FTC is ensuring that it has the tools necessary to respond to the growth of mobile commerce and conduct mobile-related investigations. In the past month, the FTC has expanded its Internet lab to include smartphone devices on various platforms and carriers. The Commission also has obtained the equipment necessary to collect and preserve evidence from these mobile devices. With these smartphones, FTC staff can now improve its monitoring of unfair and deceptive practices in the mobile marketplace, conduct research and investigations into a wide range of issues, and stay abreast of the issues affecting teens and all consumers.

### *C. P2P File-Sharing*

P2P file-sharing allows people to share their files through an informal network of computers running the same software. Teens use P2P programs to share music, games, or software online. However, P2P file-sharing presents privacy and security

---

should be easier for consumers to exercise choice. For example, rather than burying important choices in a lengthy privacy policy, such choices should be presented at the most relevant time—*e.g.*, the point of information collection or use. Further, it may not be necessary to provide choice about uses of data that are implicit or expected as part of a transaction—for example, sharing address information with a shipping company to send a product that the consumer has requested. Finally, participants noted that companies should build basic privacy protections into their systems at the outset by, for example, collecting and retaining information only if they have a business need to do so. The Commission is taking these basic principles into account as it develops privacy proposals to be released for comment later this year.

<sup>22</sup> In addition to the information presented at the roundtables, the Commission received over 100 submissions in response to its request for written comments or original research on privacy, available at [www.ftc.gov/os/comments/privacyroundtable/index.shtm](http://www.ftc.gov/os/comments/privacyroundtable/index.shtm).

<sup>23</sup> Amanda Lenhart, Rich Ling, Scott Campbell, Kristen Purcell, Pew Internet & American Life Project, *Teens and Mobile Phones* (Apr. 20, 2010), available at [www.pewinternet.org/~media/Files/Reports/2010/PIP-Teens-and-Mobile-2010.pdf](http://www.pewinternet.org/~media/Files/Reports/2010/PIP-Teens-and-Mobile-2010.pdf).

<sup>24</sup> *Id.*

<sup>25</sup> Nielsen, *How Teens Use Media* (June 2009), available at [blog.nielsen.com/nielsenwire/reports/nielsen\\_howteensusemedia\\_june09.pdf](http://blog.nielsen.com/nielsenwire/reports/nielsen_howteensusemedia_june09.pdf).

<sup>26</sup> Under the rulemaking authority granted to it by the Children's Online Privacy Protection Act of 1998 ("COPPA"), the FTC promulgated the COPPA Rule, 16 CFR Part 312, in 1999.

risks because consumers may unknowingly allow others to copy private files they never intended to share. The FTC has sought to address these risks in several ways.

First, the Commission has undertaken an initiative targeting businesses that use or allow P2P programs on their networks without implementing reasonable safeguards to protect their customers' information from inadvertent disclosure through these programs. This customer information can be leaked onto a P2P network when, for example, an employee downloads a P2P program directly onto his or her work computer, or when a business chooses to utilize P2P file-sharing programs, but does not configure its network correctly to protect such information.

To address this problem, the Commission recently sent letters notifying several dozen public and private entities—including businesses, schools, and local governments—that customer information from their computers had been made available on P2P file-sharing networks.<sup>27</sup> In the notification letters, the FTC urged the entities to review their security practices, explained that they should take steps to control the use of P2P software on their networks, and shared new business education materials designed to help them protect their confidential data from inadvertent sharing to a P2P network.<sup>28</sup> Many entities that received these notifications contacted FTC staff for additional information to aid in their investigations into the file-sharing incidents, and a number reported making changes to their security practices to prevent inadvertent file-sharing to P2P networks. At the same time it sent the notification letters, the FTC opened non-public investigations into other companies whose customer or employee information had been exposed on P2P networks.<sup>29</sup>

FTC staff has also assisted P2P file-sharing software developers in devising best practices to help prevent consumers from inadvertently sharing personal or sensitive data over P2P networks. In July 2008, the Distributed Computer Industry Association published voluntary best practices to guard against inadvertent file sharing. With the assistance of an independent P2P technology expert, FTC staff have been assessing whether members are complying with these best practices.

The FTC also seeks to educate consumers about the risks of P2P file sharing software. Among other things, the agency provides tips for consumers about P2P in a consumer alert entitled “P2P File-Sharing: Evaluate the Risks,”<sup>30</sup> which is available through *OnGuardOnline.gov*, and in *Net Cetera*.

Finally, the FTC has brought enforcement actions alleging that certain P2P file sharing software providers made deceptive claims in connection with the marketing of their products.<sup>31</sup>

## V. Privacy Models and Teens

The issues surrounding teens' use of digital technology raise the question whether there should be special privacy protections for them. Some have suggested that COPPA's protections be extended to cover adolescents between the ages of 13 and 18; others suggest that separate privacy protections should be established for teens.<sup>32</sup>

The COPPA statute and implementing regulations enforced by the FTC require operators to provide notice to, and receive consent from, parents of children under age 13 prior to the collection, use, or disclosure of such children's personal information on websites or online services. In the course of drafting COPPA, Congress looked closely at whether adolescents should be covered by the law, ultimately deciding to define a “child” as an individual under age 13. This decision was based

<sup>27</sup> FTC Press Release, *Widespread Data Breaches Uncovered by FTC Probe*, (Feb. 22, 2010), available at [www.ftc.gov/opa/2010/02/p2palert.shtm](http://www.ftc.gov/opa/2010/02/p2palert.shtm).

<sup>28</sup> These materials are available at [www.ftc.gov/bcp/edu/pubs/business/idtheft/bus46.shtm](http://www.ftc.gov/bcp/edu/pubs/business/idtheft/bus46.shtm).

<sup>29</sup> FTC Press Release, *supra* note 27.

<sup>30</sup> The consumer alert is available at [www.ftc.gov/bcp/edu/pubs/consumer/alerts/alt128.shtm](http://www.ftc.gov/bcp/edu/pubs/consumer/alerts/alt128.shtm).

<sup>31</sup> *FTC v. Cashier Myricks Jr.*, Civ. No. CV05-7013-CAS (FMOx) (C.D. Cal., filed Sep. 27, 2005) (suit against the operator of the website MP3DownloadCity.com for making allegedly deceptive claims that it was “100 percent LEGAL” for consumers to use the file-sharing programs he promoted to download and share music, movies, and computer games); *FTC v. Odysseus Marketing, Inc.*, Civ. No. 05-330 (D.N.H., filed Sep. 21, 2005) (suit against website operator that encouraged consumers to download free software falsely marketed as allowing consumers to engage in anonymous P2P file-sharing).

<sup>32</sup> See Hearing: an Examination of Children's Privacy: New Technologies and the Children's Online Privacy Protection, Prepared Statement of Professor Kathryn Montgomery Before the Subcommittee on Consumer Protection, Product Safety, and Insurance, Committee on Commerce, Science, and Transportation, U.S. Senate (Apr. 29, 2010), available at [www.democratiamedia.org/files/u1/2010-04-28-montgomerytestimony.pdf](http://www.democratiamedia.org/files/u1/2010-04-28-montgomerytestimony.pdf); see also An Examination of Children's Privacy: New Technologies and the Children's Online Privacy Protection Act (COPPA), Prepared Statement of Marc Rotenberg, EPIC.org, available at [epic.org/privacy/kids/EPIC\\_COPPA\\_Testimony\\_042910.pdf](http://epic.org/privacy/kids/EPIC_COPPA_Testimony_042910.pdf).

in part on the view that most young children do not possess the level of knowledge or judgment to make appropriate determinations about when and if to divulge personal information over the Internet. The FTC supported this assessment.<sup>33</sup>

While this parental notice and consent model works fairly well for young children, the Commission is concerned that it may be less effective or appropriate for adolescents. COPPA relies on children providing operators with parental contact information at the outset to initiate the consent process. The COPPA model would be difficult to implement for teens, as they have greater access to the Internet outside of the home than young children do, such as in libraries, friends' houses, or mobile devices. Teens seeking to bypass the parental notification and consent requirements may also be less likely than young children to provide accurate information about their age or their parents' contact information. In addition, courts have recognized that as children age, they have an increased constitutional right to access information and express themselves publicly.<sup>34</sup> Moreover, given that teens are more likely than young children to spend a greater proportion of their time online on websites that also appeal to adults, the practical difficulties in expanding COPPA's reach to adolescents might unintentionally burden the right of adults to engage in online speech.<sup>35</sup>

The Commission will continue to evaluate how best to protect teens in the digital environment and take appropriate steps to do so. In specific instances, there may be opportunities for law enforcement or advocacy in this area. For example, just this week, the Commission's Bureau of Consumer Protection sent a letter to individual stakeholders in XY corporation, which operated a now-defunct magazine and website directed to gay male youth. The letter expressed concern about these individuals' efforts to obtain and use old subscriber lists and other highly sensitive information—including names, street addresses, personal photos, and bank account information from gay teens. The letter warns that selling, transferring, or using this information would be inconsistent with the privacy promises made to the subscribers, and may violate the FTC Act; thus, the letter urges that the data be destroyed.

More generally, the FTC believes that its upcoming privacy recommendations based on its roundtable discussions will greatly benefit teens. The Commission expects that the privacy proposals emerging from this initiative will provide teens both a greater understanding of how their data is used and a greater ability to control such data. Finally, the Commission is available to work with this committee, if it determines to enact legislation mandating special protections for teens.

## VI. Conclusion

The Commission is committed to protecting all consumers in the digital environment, especially those consumers, such as teens, who are particularly vulnerable to threats on the Internet. The FTC will continue to act aggressively to protect teens through education, law enforcement, and policy initiatives that will better enable teens to control their information online.

Thank you for this opportunity to discuss the privacy and security of teens on the Internet. I look forward to your questions.

Senator PRYOR. And thank you.

At this point, since I just have a couple of minutes left in the rollcall, I will recess the hearing, and we'll reconvene when—hopefully, I'll be back in just 10 minutes or so. I mean—but, as soon as one of us gets back, we'll reconvene the hearing, and we'll hear from the rest of the panel.

And look forward to that. And thank you, again.

[Recess.]

Senator PRYOR. I'll go ahead and reconvene the Subcommittee.

<sup>33</sup> See Testimony of the Federal Trade Commission Before the Subcommittee on Communications, Senate Committee on Commerce, Science, and Transportation (Sept. 23, 1998), available at [www.ftc.gov/os/1998/09/priva998.htm](http://www.ftc.gov/os/1998/09/priva998.htm).

<sup>34</sup> See, e.g., *American Amusement Mach. Ass'n v. Kendrick*, 244 F.3d 572 (7th Cir. 2001) (citing *Erznoznik v. city of Jacksonville*, 422 U.S. 205, 212–14 (1975); *Tinker v. Des Moines Independent School District*, 393 U.S. 503, 511–14 (1969)).

<sup>35</sup> See *ACLU v. Ashcroft*, 534 F.3d 181, 196 (3d Cir. 2008) (citing *ACLU v. Gonzales*, 478 F. Supp. 2d 775, 806 (E.D. Pa. 2007) (“Requiring users to go through an age verification process would lead to a distinct loss of personal privacy.”)); see also *Bolger v. Youngs Drug Prods. Corp.*, 463 U.S. 60, 73 (1983) (citing *Butler v. Michigan*, 352 U.S. 380, 383 (1957) (“The Government may not reduce the adult population . . . to reading only what is fit for children.”)).

Again, thank you all for your patience. We had two votes. And I talked to at least a couple of my colleagues that said they're heading over here, maybe more. But, if we can, let's go ahead and pick up with where we were.

And, Mr. Nigam, go ahead, please. Thank you.

**STATEMENT OF HEMANSHU NIGAM, CO-CHAIR, ONLINE SAFETY TECHNOLOGY WORKING GROUP; SAFETY ADVISOR, NEWS CORPORATION; AND FOUNDER, SSP BLUE**

Mr. NIGAM. Chairman Pryor, thank you for giving me the opportunity to address you today on the best ways that we can, collectively, protect youth online.

My name's Hemanshu Nigam, and I bring over 20 years of experience in the safety worlds in the online and offline sites. I'm the Founder of SSP Blue, a safety, security, and privacy strategic consulting business, and a board member of the National Center for Missing and Exploited Children. I'm also a News Corporation Safety Advisor, having previously been MySpace's Chief Security and Safety Officer. Before News, I led Microsoft's child safety and cyberenforcement teams, and, prior to that, was Vice President of Worldwide Internet Enforcement at MPAA. I have also served as a Department of Justice prosecutor against Internet child exploitation and computer crimes, advised the COPA Commission and advised the White House on cyberstalking. Finally, I began my career as a prosecutor in the Los Angeles County District Attorney's Office, where I specialized in prosecuting child molestation and sex crime cases.

And so, I speak to you from various perspectives in the private sector, in government, and law enforcement. As Co-Chair of the Online Safety Technology Working Group, I led the review and evaluation of industry efforts in four key areas: online safety, education, and awareness; reporting of child pornography; data retention; and online safety technologies. The OSTWG had representatives from nearly every facet of the online safety—child safety ecosystem who brought more than 250 years of experience to the table.

Our goal is to find holistic solutions to what is a multidimensional challenge. We built upon the teachings of previous online safety task forces that have occurred over the past 10 years by inviting experts to inform our subcommittees on the latest online safety developments. From the breadth and depth of the 39 recommendations—in case you were wondering how many there actually were—from the breadth and depth of the 39 recommendations we make in our report, “Youth Safety in a Living Internet,” I think we succeeded in meeting our goal.

And before I share some of these recommendations, I'd like to talk about one concept that became quite clear. As we state in the report, the Internet is a living thing that constantly mirrors our society, our lives, and our publications. And, as such, we have to treat safety online in much the same way as we treat safety offline. And just as it takes a village to raise a child in the physical world, it takes the same village to raise a child in the online world. And given its dynamic nature, there is no one-size-fits-all solution and no silver bullet, just like in the physical world. Not surprisingly,

our children seem to know how our offline and online worlds are intertwined far better than we adults do.

And it is with full recognition of this living Internet that we make our recommendations to you. And here is just a sampling:

The Subcommittee on Internet Safety Education recommended that an online research database be created and better coordination of the multitude of Federal Government educational efforts be done.

The Subcommittee on Parental Controls and Child Protection Technology recommended that a common set of terms be created to help parents understand the various tools better, and that these technologies be baked into online products, where possible.

The Subcommittee on Child Pornography Reporting recommended that smaller service providers be helped by the larger industry, folks like ourselves, to get them to comply with reporting requirements. This subcommittee also recommended tax credits for industry to offset the high development costs of reporting.

Finally, the Subcommittee on Data Retention recommended that the discourse about data retention be held at the Federal level and that Congress take a closer look at data preservation before considering mandatory data retention.

And, just as we observed that the Internet had evolved from merely a technical tool to a reflection of our living society, we also became markedly aware of two important areas that require congressional action:

First, create a cross-functional, cross-agency coordinating body, led by the government, that includes members from every sector of the child safety ecosystem, to build consensus and coordinate education efforts.

Second, enact legislation that would require a review of all the online safety-related programs the Federal Government has already undertaken in order to evaluate their effectiveness.

We in the industry must be a critical part of solutions, as well. Having led safety efforts at MySpace, I'd like to offer you examples of just how the industry should take a holistic approach to online safety by building programs that consist of safety technologies, education, collaboration, and enforcement.

As builders of technological platforms, MySpace provides both front-end user tools and back-end member protections. We give users the ability to block other users to reduce incidents of cyberbullying. We also review images to keep out unwanted content.

Technical solutions must be coupled with educational programs that raise awareness about safety online. MySpace has distributed safety guides to over 55,000 schools in this country, and has an informative safety section on its site for all visitors.

The industry must also collaborate with child safety experts. And we've partnered with leading child advocacy organizations in the country, like the National Center. These partnerships have been used to protect children, assist in recovering runaways, and preventing suicides.

At the end of the day, as you know, Mr. Chairman, as former Attorney General of Arkansas, illegal incidents can and do occur;

thus, we work closely with law enforcement—24 hours, 7 days a week—to help ensure the safety of our users.

And speaking more broadly, and as I close, Congress also has a critical role to play in protecting children online:

First, we ask that you convene the experts. Today’s hearing is a great example of a place where we can identify problems and cutting-edge solutions.

Second, educate the masses. The more we can implement educational programs at every level of our education system, the healthier our citizens will be online.

And third, fund online safety programs. A solution, without proper funding is, frankly, no solution at all.

So, thank you, Chairman Pryor, Chairman Rockefeller, and Ranking Member Wicker, for giving me this opportunity to address you on this important topic.

[The prepared statement of Mr. Nigam follows:]

PREPARED STATEMENT OF HEMANSHU NIGAM, CO-CHAIR, ONLINE SAFETY TECHNOLOGY WORKING GROUP; SAFETY ADVISOR, NEWS CORPORATION; AND FOUNDER, SSP BLUE

Chairman Pryor, Ranking Member Wicker, and members of the Subcommittee, thank you for giving me the opportunity to address you today on the best ways that we can collectively protect youth online. I bring with me over 20 years of experience in safety in the online and offline worlds. I am the Founder of SSP Blue, a safety, security, and privacy strategic consulting firm for online businesses. I am also News Corporation’s Safety Advisor, having previously served as News Corporation and MySpace’s Chief Security Officer from the birth of social media. Before coming to News Corporation, I set in motion a cross-company strategy for child safe computing and led a cyber enforcement team at Microsoft Corporation. And prior to that, I was Vice President of Worldwide Internet Enforcement against digital movie piracy at the Motion Picture Association of America. I have also served as a Federal prosecutor against Internet child exploitation and computer crimes at the U.S. Department of Justice, an advisor to the COPA Commission, and an advisor to the White House’s Committee on Cyberstalking. Finally, I began my career as a prosecutor in the LA County District Attorney’s office, specializing in child molestation and sex crimes cases. And so, I speak to you from various perspectives in private industry, government, and law enforcement.

As co-chair of the Online Safety Technology Working Group, I had the honor of leading the mandate to review and evaluate:

1. The status of industry efforts to promote online safety through educational efforts, parental control technology, blocking and filtering software, age-appropriate labels for content or other technologies or initiatives designed to promote a safe online environment for children;
2. The status of industry efforts to promote online safety among providers of electronic communications services and remote computing services by reporting apparent child pornography, including any obstacles to such reporting;
3. The practices of electronic communications service providers and remote computing service providers related to record retention in connection with crimes against children; and
4. The development of technologies to help parents shield their children from inappropriate material on the Internet.

The OSTWG had representatives from nearly every facet of the child online safety ecosystem totaling more than 250 years of experience in online safety. Members were appointed from the Internet industry, child safety advocacy organizations, educational and civil liberties communities, the government, and law enforcement communities.

In order to best identify the best solutions for protecting youth online, the OSTWG quickly created four subcommittees to focus on each area we were asked to evaluate. These subcommittees were chaired as follows: Lawrence J. Magid of Connect Safely led the Education subcommittee; Michael W. McKeenan of Verizon led the Data Retention subcommittee; Christopher G. Bubb of AOL led the Child

Pornography Reporting subcommittee; and Adam Thierer of the Progress and Freedom Foundation led the Technology subcommittee. Given the deadline of providing a report to Congress within 1 year of the first meeting, we set and followed a very strict timeline that began with an introductory meeting on June 4, 2009. We then held meetings at which each subcommittee invited experts to provide valuable insights to inform the work of that particular subcommittee. Each subcommittee meeting also began with a special guest who provided context for the day.

Our goal was to provide holistic solutions to the multidimensional challenge of protecting youth online. This was accomplished by building upon the teachings of three task force reports issued over the prior 10 years—the COPA Commission report, the “Thornburgh report,” and the Harvard University Berkman Center Internet Safety and Technical Task Force report—and hearing from every aspect of the child safety ecosystem. From the breadth and depth of the 39 recommendations we made in our report, “*Youth Safety on a Living Internet*,” I think we succeeded in meeting our goal.

Before I share these specific recommendations, I want to share one concept that became quite clear as a result of this engaging process. As we say in the first line of the report, the Internet is a living thing that reflects at any given moment in time our humanity’s lives, sociality, publications and productions. It is very much a part of our lives and similarly our lives are very much a part of it. As such, users online are intertwined with and often responsible for their own safety in this living thing. And given its dynamic nature, there is no one-size-fits-all solution and no silver bullet. Finally, our youth recognize how our offline and online worlds are intricately intertwined far better than we adults do.

It is with full recognition of this moving, living, breathing medium that we make our recommendations.

Instead of repeating the Subcommittee reports in its entirety, here are some key recommendations that came from the work of each subcommittee.

The Subcommittee on Internet Safety Education found that applying the Primary/Secondary/Tertiary models used in risk prevention programs would work well in Internet safety programs, especially since a high correlation exists between offline and online risk. Thus, this subcommittee recommended in part that a continually updated online research database is necessary, as is the need to coordinate the multitude of Federal Government educational efforts in progress.

The Subcommittee on Parental Controls & Child Protection Technology found that a diverse array of protective tools is available today. These tools are most effective as part of a “layered” approach to child online safety especially one that supplements parental education. Thus, this subcommittee recommended that a common set of terms be created to help parents understand the various tools better and that these technologies be “baked” into online products where possible.

The Subcommittee on Child Pornography Reporting found that the PROTECT Our Children Act of 2008 had made marked improvements in the child pornography reporting process having instant impact on the volume of reports being made by the online industry to the National Center for Missing and Exploited Children. Yet, nascent and smaller service providers need to be brought into the reporting fold. Thus, the subcommittee recommended that these smaller providers be helped along by the larger industry and work more closely with NCMEC. The subcommittee also recommended the consideration of tax credits for industry given the high development cost of proper reporting and data protection.

Finally, the Subcommittee on Data Retention highlighted the multiple facets to determining what data and how much data should be retained by service providers. Varying viewpoints from the law enforcement, privacy advocacy, and industry sectors were considered. It was clear that law enforcement has a significant need for certain data to properly investigate crimes against children online. It was also clear that this need must be balanced with privacy concerns from legitimate users and the costs of data retention by service providers. Thus, the Subcommittee recommended that this discourse be maintained at the Federal level to achieve the greatest progress and that Congress take a close look at data preservation procedures enacted through the PROTECT Act before considering mandatory data retention.

These are just some of the 39 recommendations we make in the OSTWG report. Just as we observed that the Internet had evolved from merely a technical tool to a reflection of our living society, we also became markedly aware of what I consider to be 50,000 foot-level achievable recommendations for future Congresses to consider when creating task forces and working groups.

First, provide proper support and funding to task forces and working groups. Unfunded mandates quickly place undue burdens on our citizens who stand ready to serve the American public.

Second, fill the prescription that this and any working group writes by perhaps mandating a group whose sole purpose is to drive execution of the recommendations.

Third, create a cross-functional/cross-agency coordinating body led by the government with members from every sector of the child safety ecosystem to build consensus and coordinate execution efforts.

Fourth, conduct a review of all the online safety related programs the Federal Government has already undertaken and highlight the most successful ones. These programs can be a great place for public/private partnerships.

Fifth, take a multi-stakeholder approach when solving the complex issues presented by today's new media environment. The OSTWG was successful for exactly this reason.

We in the industry must be a critical part of the solutions as well.

Having led safety efforts at MySpace and News Corporation from the time that the social media industry was just an infant and before that at Microsoft Corporation, I offer you examples of just how the industry can take a holistic approach to online safety. As unusual as it may sound, the industry can find parallel and sometimes exact solutions to online challenges in the real world. Every online safety program must consist of technology, education, collaboration and enforcement designed to prevent unwanted content, contact and conduct.

As builders of these technological platforms, industry must provide both front end user tools and back end member protections. MySpace, for example, provides users the ability to block anyone from contacting them, reducing incidents of cyberbullying. MySpace also automatically locks an account that appears to have anomalous activity to prevent phishing and spam attacks against users.

The best technical solutions must then be coupled with educational programs to raise awareness about healthy online behaviors. MySpace provides guides for parents, teens and school officials with exactly this purpose. The school guides have reached over 55,000 schools in this country. MySpace also uses teachable moments across the site such as during the photo posting process where users are informed about acceptable content policies.

While industry may be expert in technology, we must collaborate with experts in other sectors of child online safety. MySpace has formed relationships with the National Center for Missing and Exploited Children, iKeepSafe, Connect Safely, and Enough is Enough—some of the leading child advocacy organizations in the country. Working with NCMEC, MySpace sends AMBER Alerts to users when a child is kidnapped or missing. MySpace also works with the National Suicide Prevention Lifeline when a user is in crisis to get them help immediately thereby preventing possible suicides.

At the end of the day, we know that illegal incidents can occur, thus working closely with law enforcement 24/7/365 is a must for all of us. MySpace works with law enforcement to respond to requests for information that might help bring a perpetrator to justice. MySpace also works with law enforcement directly to assist in runaway situations in an effort to reunite runaway teens with their families.

Thus, any industry online safety program must be holistic in nature encompassing technology, education, collaboration, and enforcement. I will say that the industry has come a long way since my own days as a child predator prosecutor in the Department of Justice.

Speaking more broadly, as this subcommittee examines Protecting Youths in an Online World, you have a significant and undeniably critical role to play that we in the industry would embrace with open arms and one that is necessary for the protection of this Nation's children online.

Convene the Experts to inspire the dialogue. Today's hearing is a great example of just this. The more places that you can inspire folks to gather, discuss, and analyze, the more pointed solutions can be identified.

Educate the Masses to increase safer online practices. The more we can mandate educational programs at every level of our education system, including colleges, the healthier our citizens will be in their daily online practices.

Fund the Programs to implement safety solutions. A perfect solution to a complex problem without proper funding is no solution at all. This is very much like recommending that students learn to read in elementary school without providing teachers and books to make that happen.

I look forward to working with this subcommittee to identify specific action items that can help you convene the experts, educate the masses and fund the programs.

In closing, I think we can step forward fully cognizant of the challenges that lie before us in protecting youth online and at the same time greatly hopeful that we

can find and implement solutions that will allow our children to grow up healthy in this digital age.

Thank you Chairman Pryor, Ranking Member Wicker, and members of the Subcommittee for giving me this opportunity address you.

Senator PRYOR. Thank you.

Mr. McIntyre.

**STATEMENT OF JEFF MCINTYRE,  
DIRECTOR—NATIONAL POLICY, CHILDREN NOW**

Mr. MCINTYRE. There we go.

Good afternoon, Chairman Pryor, Chairman Rockefeller, Ranking Member Wicker, and the other members of the Subcommittee. I'm Jeff McIntyre, and I'm the Director of National Policy for Children Now. I'm also the Chair of the Children's Media Policy Coalition, which includes the American Academy of Pediatrics, the American Psychological Association, and the National PTA.

My main concerns are children's health and education in media. The issues this subcommittee and the Online Safety and Technology Working Group report deal with are, frankly, issues we've been dealing with since well before media was prevalent in our lives: predators, bullies, invasion of our children's privacy, their information being used inappropriately, the effects of advertising on children's health. These are issues that parents are generally worried about.

So, why is it—so, why is interactive media important in this? Basic child development teaches us that children learn from the environments they are in: schools, families, religious institutions, and communities. But, according to a recent Kaiser Family Foundation report, the place where children and youth spend most of their time is in the media environment. Children spend more time immersed in media than they do in any other activity. They average just over seven and a half hours a day in nonacademic media, and just under 11 hours a day if you account for multi-tasking. In today's world, that means children and youth are spending enormous amounts of time interacting with media and the individuals behind that media.

Parents can exert great control over where a child is, geographically; but, in the interactive world, that's an immensely difficult task to do. This has been an issue, for those of us concerned about children, for years. With the introduction of television came the very first Congressional hearings on whether it contributed to juvenile delinquency back in the 1950s, violent media, sexualization, unhealthy food marketing. It's about kids receiving information detrimental to their health that is inappropriate for their developmental level.

Now it's no longer just passive watching. It's about children and youth receiving and giving and then receiving targeted, sometimes even individualized, information across platforms. Children and youth are no longer just observers of media, soaking up information like a sponge. Now they are active participants, often bypassing parents to create and remix games, websites, social networking profiles, or participate in chat rooms and advergaming. These platforms, however, are increasingly designed for the individual, and the software often tweaked for that individual. Every time a child

or youth get propositioned online, bullied, asked for inappropriate information, or sent a coupon on their wireless without their parents actively choosing for that to happen, that parent's authority has been hijacked.

It's easy to get stars in our eyes when we start talking about technology and media or the latest app, but the basics of what's healthy or harmful for our children have existed since, well, before television, and will exist long after the latest platform fad has passed. Simply put, "buyer beware" should not apply to our kids, especially in an interactive environment, not with predators in chat rooms, not with bullies, and not with advertisers using their information against them.

Let me also say that an over-reliance on media literacy as the panacea to these issues is an incomplete response. Media literacy is about education, it's about building awareness. It's something that no one is really opposed to. However, it is only a small part of the overall equation.

I think it's very important that the Subcommittee and the Committee understand that building awareness "may" result in a slow shift of attitude, which "might" influence behavior over an extended period of time, usually years or more. And even then, the amount of media literacy content is exponentially dwarfed by the amount of contrary unhealthy media content that is available and actively marketed to children and youth.

For instance, in 19—excuse me, a 2007 study showed that tweens, between the ages of 8 and 12, were exposed to almost 8,000 advertisements a year on television alone, the majority of which were for food items, such as candy and fast food; none were for healthy foods, such as fruits or vegetables. And one in five of those ads included a push to a website. And that was 3 years ago. The same group would see a public service announcement, a PSA, roughly about once every 3 days.

Our boat is small here, and the ocean of other media is wide and deep, that our children are in. Education is about citizenship, digital or otherwise. Years of Children Now research on children's media, whether the—on the effects of media duopolies on children's educational programming, the presence of minorities in children's programming, or the extreme lack of effectiveness of advertising pledges by the food and beverage companies, has demonstrated that industrywide standards tend to meet only the barest minimum dictated by that regulation. And that doesn't matter whether it's government or self-regulatory. Then they tend to punt to public affairs to attempt to shift the burden of responsible media onto the parent or child viewer.

Now, if you think of this with sexual predators, just achieving the lowest common denominator and just talking to our children about sexual predators is a very small step, but it doesn't really come close to helping solve that issue. Other protections need to be put in place to have a comprehensive, truly safe, healthy environment for our children and youth. While media education is incredibly important, it should not be a loophole for structural attention to these issues. Real demonstrated change must occur in the media environment, for our children to be truly safe.

I want to thank the members of the Subcommittee and Committee for their attention and leadership on this issue. Children Now stands ready to offer our assistance and resources as you move forward—as we move forward in addressing this critical moment in our media history.

[The prepared statement of Mr. McIntyre follows:]

PREPARED STATEMENT OF JEFF MCINTYRE,  
DIRECTOR—NATIONAL POLICY, CHILDREN NOW

Good Morning Chairman Pryor, Ranking Member Wicker and members of the Subcommittee. I'm Jeff McIntyre and I'm the Director of National Policy for Children Now. I'm also the Chair of the Children's Media Policy Coalition, which includes the American Academy of Pediatrics, the American Psychological Association, and the National PTA.

My main concerns are children's health and education—in media. The issues this Subcommittee and the Online Safety and Technology Working Group Report deal with are, frankly, issues we've been dealing with since well before media was prevalent in our children's lives. Predators, bullies, invasion of our children's privacy, their information being used inappropriately, the effects of advertising on our children's health—these are issues that all parents are worried about.

So, why is interactive media important in this? Basic child development teaches us that children learn from the environments they are in—schools, families, religious institutions, and communities. But, according to a recent Kaiser Family Foundation report—the place where children and youth spend most of their time is in the media environment. Children spend more time immersed in media than any other activity. They average just over seven and a half hours a day in non-academic media—and just under 11 hours a day, if you account for multi-tasking. In today's world, that means children and youth are spending enormous amounts of time interacting with media—and the individuals behind that media. Parents can exert great control over where a child is geographically. In the interactive world, that's an immensely difficult task to do.

This has been an issue for those concerned about children for years—with the introduction of television came the first Congressional hearings on whether it contributed to juvenile delinquency in the 1950s. Violent media, sexualization, unhealthy food marketing—it's about kids receiving information detrimental to their health that is inappropriate for their developmental level. Now, it's no longer just passive watching—it's about children and youth receiving and giving and then receiving targeted—sometimes individualized—information across platforms. Children and youth are no longer just observers of media, soaking up information like a sponge. Now, they are active participants—often bypassing parents—to create and remix—games, websites, social networking profiles, or participate in chat rooms or adver-games. These platforms, however, are increasingly designed for the individual and the software tweaked for that individual.

Every time a child or youth gets propositioned online, bullied, asked for inappropriate information, or sent a coupon on their wireless without their parents actively choosing for that to happen—that parent's authority has been hijacked. It's easy to get stars in our eyes when talking about technology, media, or the latest app. But the basics of what's healthy or harmful for our children have existed since before television and will exist long after the latest platform fad has passed. Simply put, “Buyer Beware” should not apply to our kids, especially in an interactive environment. Not with predators in chat rooms, not with bullies, and not with advertisers using their information against them.

Let me also say that an over-reliance on media literacy as the panacea to these issues is an incomplete response. Media literacy is about education—about building awareness. It is something that no one is opposed to. However, it is only a small part the overall equation. I think it's important that the Subcommittee understand that “building awareness” may result in a slow shift of attitude which might influence behavior over an extended period of time—usually years or more. And, even then—the amount of media literacy content is exponentially dwarfed by the amount of contrary, unhealthy media content available and actively marketed to children and youth.

For instance—A 2007 study showed that tweens between 8 and 12 were exposed to almost 8000 ads a year on television alone—the majority of which were for food items, such as candy and fast food. None were for healthy foods such as fruits or

vegetables. One in five ads included a push to the website. That same group would see a PSA only once every 3 days.

Our boat is small and the ocean of other media is wide and deep.

Education is about citizenship—digital or otherwise. Years of Children Now research on children’s media—whether on the effects of media duopolies on children’s educational programming, the presence of minorities in children’s programming, or the extreme lack of effectiveness of advertising pledges by the food and beverage companies—has demonstrated that industry wide standards tend to meet only the barest minimum dictated by that regulation—whether government or self-regulatory. Then, they punt to public affairs to attempt to shift the burden of responsible media onto the parent or child viewer.

If you think of this with sexual predators—just achieving the lowest common denominator and just talking to our children about sexual predators is a very small step—but it doesn’t really come close to helping solve that issue. Other protections need to be put in place to have a comprehensive, truly safe, healthy environment for our children and youth. While media education is incredibly important, it should not be a loophole for structural attention to these issues. Real, demonstrated change must occur in the media environment for our children to be truly safe.

I want to thank Chairman Pryor, Ranking Member Wicker and the Subcommittee for their attention and leadership on this issue. Children Now stands ready to offer our assistance and resources to you as we move forward in addressing this critical moment in our media history.

Senator PRYOR. Thank you.  
Ms. Collins.

**STATEMENT OF MICHELLE COLLINS, VICE PRESIDENT,  
EXPLOITED CHILDREN DIVISION, THE NATIONAL CENTER  
FOR MISSING & EXPLOITED CHILDREN**

Ms. COLLINS. Mr. Chairman and members of the Subcommittee, I welcome this opportunity to appear before you to discuss the risk to children on the Internet. The National Center for Missing & Exploited Children, NCMEC, joins you in your concern for the safety of our youth, and thanks you for bringing attention to this very serious problem facing America’s communities.

As you know, NCMEC is a not-for-profit corporation mandated by Congress and working in partnership with the U.S. Department of Justice. NCMEC is a public/private partnership funded in part by Congress and in part by the private sector. For 26 years, NCMEC has operated under Congressional mandate to serve as the Nation—or the national resource center for missing and exploited children.

This statutory mandate includes 19 specific operational functions, among which is the CyberTipline, which is the 9–1–1 of the Internet, that public and electronic service providers may use to report Internet crimes against children.

The CyberTipline is the national clearinghouse for leads and tips regarding child sexual exploitation crimes. It’s operated in partnership with Federal, State, and local law enforcement agencies, including the FBI and the Internet Crimes Against Children Task Forces that are located throughout the country. We receive reports in eight categories of crime—or crimes against children, including the possession, manufacture, and distribution of child pornography, as well as online enticement of children for sexual acts.

NCMEC is pleased to have participated in the Online Safety and Technology Working Group, OSTWG, created by this committee’s legislation. Its membership comprised a broad spectrum of knowledge and experience in online safety arena. The report recently issued by OSTWG contains important recommendations for

progress. I'd like to underscore the OSTWG's report's conclusion that approaches to online safety must take into account the dynamic nature of the Internet and technology and the way that things can be used.

We agree that everyone has a role to play. Parents and guardians can become more involved in their children's online activities, industry can actively self-regulate to keep its safe—or, its users safer, and the government can help increase awareness and encourage digital literacy. These efforts would benefit significantly from comprehensive, up-to-date information on these issues. Given the rapidly changing landscape of online communication, we strongly recommend that current research be conducted and maintained.

The Internet offers tremendous potential, especially for youth. It has changed the way we communicate, learn, and conduct our daily activities. Unfortunately, the Internet can also be used to victimize children. The combination of widespread use and relative anonymity makes it an appealing tool for those who wish to victimize children. This is supported by our data. Reports to the CyberTipline about online enticement of children for sexual acts has increased 714 percent since 1998. The attachments to my written testimony contain excerpts from actual CyberTipline reports that illustrate the problem.

Youth will often engage in risky behavior in both the real world and the online world. The combination of the Internet, easy transmission of digital images, and poor judgment can lead to serious and unintended consequences for youth, including becoming the victim of enticement, blackmail, harassment, and exploitation by both adults and other youths.

Webcams, cell phone Internet access, and social networking sites increase the vulnerability of our children. Webcams offer this exciting ability to see the person you're communicating with over the Internet. While this technology has many benefits, it can also be used, and is used, to exploit children. The reports to our CyberTipline of incidents involving children and Webcams have increased. Many children are victimized inadvertently by appearing on their Webcams without clothes as a joke or on a dare from friends, unaware that these images may end up in a global child pornography enterprise. Other children are victims of blackmail, threatened with disclosure to friends and family of his or her performance before the Webcam doesn't become more sexually explicit.

Cell phones have placed the—or, has placed the Internet basically in our children's pockets. From January of 2008 until December of 2009, there was a 650-percent increase in the number of CyberTip reports we've received in which a cell phone was used in the sexual victimization of a child.

"Sexting" is a term coined by the media that generally refers to a youth writing sexually-explicit messages and sending sexually-explicit images of themselves to their peers. This is an increasing problem that should be addressed through education of both parents and youth about the long-term consequences of apparently innocent activity amongst friends.

Social networking sites appeal to children's natural desire for self-expression. These hugely popular sites permit users to create profiles containing detailed and highly personal information about

themselves, which sometimes can lead to individuals forging relationships with that child. Children need to be taught the value of limiting access of their personal information to those who are within their known circle of family and friends.

NCMEC has two resources that can help parents and youths learn about ways to be safer on the Internet. NetSmartz is an interactive, educational safety resource for children, parents, guardians, educators, and law enforcement, that uses age-appropriate 3-D activities to teach children how to be safer on the Internet. And, NetSmartz411—it's an Internet safety help desk and online resources for parents and guardians that can help answer their questions about Internet safety.

The National Center is actively engaged with industry leaders on their efforts to make youth less vulnerable when using their services. We encourage them to prohibit illegal and abusive activity as one of their terms of services, and to enforce this vigorously.

However, the critical factor in youth online safety is parental involvement. Nothing can replace the value of parents understanding what their children are doing online, and why, and helping them develop good judgment in their online communication.

Thank you very much.

[The prepared statement of Ms. Collins follows:]

PREPARED STATEMENT OF MICHELLE COLLINS, VICE PRESIDENT, EXPLOITED CHILDREN DIVISION, THE NATIONAL CENTER FOR MISSING & EXPLOITED CHILDREN

Mr. Chairman and members of the Subcommittee, I welcome this opportunity to appear before you to discuss the risks to children on the Internet. The National Center for Missing & Exploited Children (NCMEC) joins you in your concern for the safety of our youth and thanks you for bringing attention to this serious problem facing America's communities.

As you know, the National Center for Missing & Exploited Children is a not-for-profit corporation, mandated by Congress and working in partnership with the U.S. Department of Justice. NCMEC is a public-private partnership, funded in part by Congress and in part by the private sector. For 26 years NCMEC has operated under Congressional mandate to serve as the national resource center and clearinghouse on missing and exploited children. This statutory mandate (see 42 U.S.C. § 5773) includes 19 specific operational functions, among which are:

- operating a national 24-hour toll-free hotline, 1-800-THE-LOST® (1-800-843-5678), to intake reports of missing children and receive leads about ongoing cases;
- providing technical assistance and training to individuals and law enforcement agencies in the prevention, investigation, prosecution, and treatment of cases involving missing and exploited children;
- tracking the incidence of attempted child abductions;
- providing forensic technical assistance to law enforcement;
- facilitating the deployment of the National Emergency Child Locator Center during periods of national disasters;
- working with law enforcement and the private sector to reduce the distribution of child pornography over the Internet;
- operating a child victim identification program to assist law enforcement in identifying victims of child pornography;
- developing and disseminating programs and information about Internet safety and the prevention of child abduction and sexual exploitation;
- providing technical assistance and training to law enforcement in identifying and locating non-compliant sex offenders; and
- operating the CyberTipline, the "9-1-1 for the Internet," that the public and electronic service providers may use to report Internet-related child sexual exploitation.

The CyberTipline is the national clearinghouse for leads and tips regarding child sexual exploitation crimes. It 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 Internet Crimes Against Children Task Forces (ICAC), the U.S. Secret Service, the U.S. Department of Justice's Child Exploitation and Obscenity Section, as well as other state and local law enforcement. We receive reports in eight categories of crimes against children:

- possession, manufacture and distribution of child pornography;
- online enticement of children for sexual acts;
- child prostitution;
- sex tourism involving children;
- extrafamilial child sexual molestation;
- unsolicited obscene material sent to a child;
- misleading domain names; and
- misleading words or digital images on the Internet.

These reports are made by both the public and by Electronic Service Providers, who are required by law to report to the CyberTipline. The leads are reviewed by NCMEC analysts, who examine and evaluate the content, add related information that would be useful to law enforcement, use publicly-available search tools to determine the geographic location of the apparent criminal act, and provide all information to the appropriate law enforcement agency for investigation. These reports are also triaged to ensure that children in imminent danger get first priority.

The FBI, ICE and Postal Inspection Service have "real time" access to the CyberTipline, and assign agents and analysts to work at NCMEC. In the 12 years since the CyberTipline began, NCMEC has received and processed more than 920,000 reports. To date, electronic service providers have reported to the CyberTipline more than 7.5 million images of sexually exploited children. To date, more than 35 million child pornography images and videos have been reviewed by the analysts in our Child Victim Identification Program, which assists prosecutors to secure convictions for crimes involving identified child victims and helps law enforcement to locate and rescue child victims who have not yet been identified.

NCMEC is pleased to have participated in the Online Safety and Technology Working Group (OSTWG) created by this Committee's legislation. Its membership comprised a broad spectrum of knowledge and experience in the online safety arena. The report recently issued by OSTWG contains important recommendations for progress.

I'd like to underscore the OSTWG Report's conclusion that approaches to online safety must take into account the dynamic nature of technology and the ways that it can be used. We agree that everyone has a role to play: parents/guardians can become more involved in their children's online activities; industry can actively self-regulate to keep its users safer; and the government can help increase awareness and encourage digital literacy. These efforts would benefit significantly from comprehensive, up-to-date information on these issues. Given the rapidly changing landscape of online communication, we strongly recommend that current research be conducted and maintained.

The Internet offers tremendous potential, especially for youth. It has changed the way we communicate, learn and conduct our daily activities. Unfortunately, the Internet can also be used to victimize children. The combination of widespread use and relative anonymity makes it an appealing tool for those who seek child victims.

This is supported by our own data: reports to the CyberTipline about online enticement of children for sexual acts have increased 714 percent since 1998. The attachments to my written testimony contain excerpts from actual reports that illustrate this problem.

Youth will often engage in risky behavior, in both the "real" world and in the online world. The combination of the Internet, easy transmission of digital images, and poor judgment can lead to serious and unintended consequences for youth—including becoming the victim of enticement, blackmail, harassment and exploitation by both adults and other youth. Webcams, cell phone Internet access and social networking sites increase the vulnerability of our children.

Webcams offer the exciting ability to see the person you're communicating with over the Internet. While this technology has many benefits, it can also be used to exploit children. The reports to our CyberTipline of incidents involving children and webcams have increased. Many children are victimized inadvertently, by appearing on their webcams without clothes as a joke, or on a dare from friends, unaware that

these images may end up in a global child pornography enterprise. Other children are victims of blackmail, threatened with disclosure to friends and family if his or her “performance” before the webcam doesn’t become more sexually explicit.

Cell phones have placed the Internet in our children’s pockets. From January 2008 to December 2009, there was a 650 percent increase of CyberTipline reports in which a cell phone was involved in the sexual victimization of a child. A 2008 online survey of 653 teens between the ages of 13 and 19 conducted by TRU and presented by the National Campaign to Prevent Teen and Unplanned Pregnancy and *CosmoGirl.com* found that 20 percent of teens surveyed have posted nude or seminude pictures of themselves online. In addition, 39 percent of teens surveyed have sent or posted sexually suggestive messages (text, e-mail, IM).

“Sexting” is a term coined by the media that generally refers to youth writing sexually explicit messages, taking sexually explicit photos of themselves or others in their peer group, and transmitting those photos and/or messages to their peers. This is an increasing problem that should be addressed through education of both parents and youth about the long-term consequences of apparently “innocent” activity among friends.

Social networking sites appeal to children’s natural desire for self-expression. These hugely popular sites permit users to create online profiles containing detailed and highly personal information—which can sometimes be used by individuals to forge a “cyber-relationship” that can lead to a child being victimized. Children need to be taught the value of limiting access to their personal information to only those who are in their known circle of friends and family.

NCMEC has two resources that can help parents and youth learn about ways to be safer on the Internet:

- NetSmartz is an interactive, educational safety resource for children, parents, guardians, educators, and law enforcement that uses age-appropriate, 3-D activities to teach children how to stay safer on the Internet.
- NetSmartz411 is an Internet Safety Helpdesk, an online resource for parents and guardians that can answer questions about Internet safety, computers, portable communications devices, and much more.

NCMEC is actively engaged with industry leaders on their efforts to make youth less vulnerable when using their services. We encourage them to prohibit illegal and abusive activity as one of their terms of service and to enforce this vigorously. It is important for them to take reports of abuse by their users and to make their users aware of this reporting ability.

However, the critical factor in youth online safety is parental involvement. Nothing can replace the value of parents understanding what their children are doing online, and why, and helping them develop good judgment in their online communications.

Thank you.

Senator PRYOR. Thank you.  
Mr. Snowden.

**STATEMENT OF K. DANE SNOWDEN, VICE PRESIDENT,  
EXTERNAL AND STATE AFFAIRS,  
CTIA—THE WIRELESS ASSOCIATION®**

Mr. SNOWDEN. Good afternoon, Chairman Pryor, Ranking Member Wicker, Chairman Rockefeller, and Senator Klobuchar.

My name is Dane Snowden, and, as the Vice President of External and State Affairs at CTIA, I was the wireless industry representative on the NTIA Online Safety and Technology Working Group. Thank you for affording me this opportunity to share CTIA’s views on protecting youth in an online and mobile world.

Across a diverse wireless ecosystem, the wireless industry is proactively doing its part to augment the educational and social growth of today’s youth by preparing them for an increasingly digitized and mobile future. CTIA is proud of the wireless industry’s commitment to make mobile safety and responsible use a priority.

With respect to the Working Group's report, we support the recommendations regarding online safety education, parental control tools, and child pornography reporting and data retention issues. Specifically, we agree that there is no one-size-fits-all, once-and-for-all solution to every aspect of online safety, especially in the rapidly innovating wireless industry.

There are several areas of the Working Group's report which I would like to highlight today. First, it will come as no surprise to every parent in the room that wireless devices are omnipresent with American teens and tweens, who often seem to communicate with text messaging, photo and video sharing, more than they do the old-fashioned way, by voice. That, I suppose, is a sign of the times.

However, we recognize that the many advantages wireless provides also present opportunities for inappropriate behavior, such as texting while driving, sexting, and cyberbullying. In a sense, this is not new behavior, and the introduction of new technology has often raised parental and policymaking concerns about the impact of that technology on young people.

As innovation in the wireless industry expanded exponentially, we anticipated that these same concerns would be raised, and have worked to stay ahead of them. In 2004, CTIA developed carrier content and Internet guidelines. Our goal was to provide consumers with information and tools to make informed choices when accessing wireless content. Fast forward to today, we see a demand for more content available via the Internet versus the old walled-garden approach.

The wireless industry has responded, and currently a majority of the 600 unique devices available can access the open Internet. In response to the evolution, the wireless industry has taken action to empower parents with choice and control over mobile wireless content so that parents may determine what is appropriate for their children.

Some of the tools our members offer include: content filters, based on rating for music, games, and apps; limits on calling, texting, and camera features; and parental notification and monitoring services. In addition, CTIA has worked to extend this successful self-regulatory model to location-based services, common short codes, and mobile financial services.

Built on notice and consent policies, CTIA's LBS guidelines promote and protect user privacy, especially for children, as innovative LBS services are developed and deployed.

Given the growing variety of devices and services capable of Internet access, it is worth noting that the Working Group's consensus is that there is no single one-size-fits-all parental-control technology or safeguard for all media platforms. Instead, as the Working Group recommended, CTIA recognizes the education and awareness-building efforts are absolutely crucial to helping parents navigate the diverse parental-control marketplace and keep up with their children's evolving mobile usage.

For this reason, CTIA and the Wireless Foundation recently launched "Be Smart. Be Fair. Be Safe: Responsible [Wireless] Use," a national education campaign to help teach children responsible

wireless-use techniques and link parents to the available tools and services offered by our member companies.

And consistent with our belief that education is key, we support legislation, offered by Senator Menendez and Representative Wasserman-Schultz, which provides government grants to a variety of stakeholders who promote Internet safety, digital citizenship, and media literacy.

As proud as we are of our efforts to date, we also know that our work to promote online safety will not be finished anytime soon, as a new cohort of users signs on, each and every day. It is our hope that the Working Group's report, along with our industry's efforts, will help to inform online safety initiatives at the Federal, State, and local levels.

The wireless industry believes that, with strategic collaborations, we will continue to meet the demand and ensure the benefits of wireless to the ever-growing list of American wireless consumers. We look forward to working with the Committee and other stakeholders to craft policies which properly balance the goal of online safety and the need for flexibility in responding quickly to behavioral, technological, and market changes.

Thank you. And I look forward to answering any questions you have.

[The prepared statement of Mr. Snowden follows:]

PREPARED STATEMENT OF K. DANE SNOWDEN, VICE PRESIDENT,  
EXTERNAL AND STATE AFFAIRS, CTIA—THE WIRELESS ASSOCIATION®

Good afternoon, Chairman Pryor, Ranking Member Wicker, and members of the Subcommittee. My name is K. Dane Snowden, and I am the Vice President of External and State Affairs at CTIA—The Wireless Association® (“CTIA”). Before joining CTIA, I was Chief of the Consumer and Governmental Affairs Bureau at the Federal Communications Commission (“FCC”) for 4 years. In my capacity at the FCC, I oversaw all agency consumer related policy issues ranging from the creation of the National Do-Not-Call regulatory policy to the consumer outreach and complaint divisions. Thank you for affording me this opportunity to share with you the views of CTIA and our member companies on protecting youth in an online world.

Today, my comments will highlight the wireless industry's continuing efforts to empower parents, safeguard privacy, and help ensure America's children and teens are using their wireless devices in a responsible manner. Through a diverse wireless ecosystem of service providers, device manufacturers, and software and application developers, the wireless industry is proactively facilitating the educational and social growth of today's youth by preparing them for an increasingly digitized and mobile future. Mobile technology offers many benefits to children and teens, including thousands of applications (“apps”) focused on civic, educational, health care and social opportunities. Even with the challenge of protecting children in the more “open” mobile wireless ecosystem, the wireless industry continues to empower parents with choice and control over mobile content so that they may determine appropriate mobile uses for their children and encourage responsible behavior. The wireless industry also has launched a series of educational initiatives and partnerships designed to promote mobile safety and responsible use.

Given the wireless industry's substantial ongoing efforts, CTIA and our member companies support Congressional efforts which encourage stakeholders to educate parents and children regarding responsible mobile device practices. As an active member of the U.S. Department of Commerce National Telecommunications & Information Administration's (“NTIA”) Online Safety and Technology Working Group (“Working Group”), CTIA also supports the *Youth Safety on a Living Internet* (“OSTWG Report”) report's findings that there is no “one-size-fits-all, once-and-for-all solution” to every aspect of online safety, rather there must be a layered, multi-

stakeholder approach which utilizes available content control tools and enhances on-line safety educational strategies for children and parents.<sup>1</sup>

**I. Children Are Using Mobile Devices and Services to Access Internet Content and Utilize Numerous Innovative Benefits on a Regular Basis**

CTIA recognizes the increasingly prominent and common role that wireless devices and services are playing in the development of America's youth. Children are actively using mobile devices on a regular basis, and progressively using mobile phones at younger ages. According to an April 2010 report by the Pew Internet & American Life Project, 83 percent of 17-year-olds now own a cell phone (up from 64 percent in 2004), and 58 percent of 12-year-olds now own a cell phone (up from 18 percent in 2004).<sup>2</sup> These children view mobile devices as critical tools for meeting their communications needs and a "centerpiece in teen social life" through text messaging, photo and video sharing, Internet access, "apps", and other mobile data services.<sup>3</sup> In addition, a mobile device may often be the only link to the Internet for children from low-income or minority homes where home broadband adoption is generally lower than other demographic communities.<sup>4</sup>

As part of this surge in children's mobile technology use, all elements of the wireless ecosystem, including carriers, manufacturers, and software and application developers, have enabled numerous innovative and beneficial tools for children, from education to health care to safety and civic participation. Using "mLearning" as just one example, innovative mobile wireless services offer personalized educational benefits as children use mobile devices to harness information on the Internet, choose from the thousands of educational "apps," and participate in class through text messaging, online polling and other multi-media uses. In fact, an entire segment of the mobile device market dedicated entirely to promoting reading through "e-readers" and downloadable books has recently developed.

It is not hard to imagine that one day soon mobile devices may replace students' traditional "book bags." Indeed, today millions of school-age children never leave home for school without a hand-held mobile device. And while some parents insist on this for safety reasons, the versatility of mobile devices for recreation as well as communication ensures that few kids need to be convinced to carry one to and from school. Despite their popularity with students, however, the utility of mobile devices as part of the educational mission has not been widely appreciated, and school administrators occasionally bemoan their potentially distracting influences. Unfortunately, this perception overlooks the vast educational benefits of mobile devices discussed above.

In order to address these issues, the *OSTWG Report* recommends policies and incentives to support "digital citizenship" which encourages children to respect themselves and others online and off and "media literacy" which promotes critical thinking about what is posted, shared, produced and uploaded as well as content that's consumed.<sup>5</sup> In addition, CTIA recommends that government agencies help ensure parents, teachers, and children take advantage of the learning opportunities provided by mobile devices, including updating school technology policies to more fully utilize mobile and Internet services and modify Federal Universal Service programs to be more technology neutral.<sup>6</sup> As mobile devices and services become more ubiquitous among America's children and teens, Congress should consider these recommendations which can help provide guidance in the evolving online mobile environment which children are increasingly and regularly utilizing.

<sup>1</sup>National Telecommunications and Information Administration, *Youth Safety on a Living Internet: Report of the Online Safety and Technology Working Group* (June 4, 2010), available at [http://www.ntia.doc.gov/reports/2010/OSTWG\\_Final\\_Report\\_060410.pdf](http://www.ntia.doc.gov/reports/2010/OSTWG_Final_Report_060410.pdf) ("OSTWG Report").

<sup>2</sup>Pew Internet & American Life Project, *Teens and Mobile Phones* (April 20, 2010), available at <http://www.pewinternet.org/Reports/2010/Teens-and-Mobile-Phones.aspx> ("Pew Teens and Mobile Phones Report").

<sup>3</sup>Comments of CTIA—The Wireless Association®, MB Docket No. 09–194 (filed Feb. 24, 2010) ("CTIA Empowering Parents NOI Comments"); see also, Pew Internet & American Life Project, *Teens and Sexting 2* (Dec. 15, 2009), available at [http://www.pewinternet.org/~media/Files/Reports/2009/PIP\\_Teens\\_and\\_Sexting.pdf](http://www.pewinternet.org/~media/Files/Reports/2009/PIP_Teens_and_Sexting.pdf) ("Pew Sexting Report").

<sup>4</sup>CTIA Empowering Parents NOI Comments at 8.

<sup>5</sup>OSTWG Report at 31–34.

<sup>6</sup>CTIA Empowering Parents NOI Comments at 13–20.

## II. The Wireless Industry Continues Proactive Efforts to Empower Parents and Encourage Responsible Use

### *a. The Wireless Industry Has Proactively Offered Tools and Developed Best Practices to Empower Parents and Protect Children*

The wireless industry has taken action to empower parents with choice and control over mobile wireless content so that they may determine what is appropriate for their children. Carriers, moreover, have taken extensive steps to meet the demands of parents for these tools and have introduced a series of initiatives to educate parents and children about the responsibilities and risks of mobile connectivity. In the “open” mobile wireless ecosystem, the *OSTWG Report* found that children are increasingly exposed to the same risks faced across other technological platforms, even as many of those risks are similar to ones they face offline.<sup>7</sup>

In response to consumer and governmental demand for open access, open devices, and greater Internet connectivity on handsets, carriers have moved away from “walled garden” approaches which offered consumers service provider-reviewed services and protected consumers, including children, from harmful content and online activities. Today, wireless carriers generally have little control over content consumers may access on their networks in the “open” wireless ecosystem. Instead, numerous entities in the wireless ecosystem create, distribute, and manage content that can be accessed by consumers, including children. As a result, children may be exposed to the same questionable content that is available on the open Internet including violent, offensive and adult-themed content, personalized advertising, privacy risks and the plethora of mobile applications which are not intended for use by children. In addition, the technological advantages of mobile previously highlighted which have opened doors for positive educational and social interactions also present opportunities for children to engage in irresponsible or inappropriate behavior on mobile devices and services, such as texting while driving, sexting, textual harassment and cyberbullying.

In addressing these issues, CTIA plays a key role in facilitating industry discussions about mobile safety and responsible use through voluntary, self-regulatory best practices and guidelines under which carriers, manufacturers and application vendors agree to provide significant protections for consumers and, most specifically, children. In 2004, well before the influx of wireless data services, applications and video services, CTIA developed *Guidelines for Carrier Content Classification and Internet Access* to provide consumers with information and tools to make informed choices when accessing wireless content.<sup>8</sup> Under these voluntary guidelines, participating carriers agree to develop content classification standards and educate consumers about the meaning of the chosen categories and ratings. While the implementation of advanced parental control technologies is left to individual wireless providers and third-party application vendors, the guidelines play an important role in providing a set of baseline requirements that help standardize content classifications for the carrier-content available on wireless devices. This in turn facilitates outreach and educational campaigns intended to inform parents about the types of content accessible via wireless devices, as well as the tools available to offer children a safe user experience.

Today, individual wireless carriers offer parents a variety of tools that can control children’s access to certain content (*e.g.*, filters) and prevent the distribution or receipt of inappropriate content (*e.g.*, feature or service limits); educate children and parents about how to be safe online; and provide parents with options to manage their children’s messaging, calling, and data usage.<sup>9</sup> Product manufacturers have also deployed effective parental and content controls to help protect children.<sup>10</sup> In addition to carrier-provided advanced technologies and parental controls, consumers today can independently download third-party solutions to their wireless devices through app stores, websites, and other outlets, opening up a host of additional con-

<sup>7</sup> *OSTWG Report* at 5.

<sup>8</sup> Wireless Content Guidelines, CTIA Consumer Info, [http://www.ctia.org/consumer\\_info/service/index.cfm/AID/10394](http://www.ctia.org/consumer_info/service/index.cfm/AID/10394) (last visited June 28, 2010) (“Guidelines for Carrier Content Classification and Internet Access”).

<sup>9</sup> FCC, *Implementation of the Child Safe Viewing Act; Examination of Parental Control Technologies for Video or Audio Programming*, Report, MB Docket 09–26, ¶99 (2009) (“FCC Child Safe Viewing Act Report”).

<sup>10</sup> For example, the Apple iTunes and App Stores include content-based age ratings for apps, and the iPhone and iPad allow users to restrict apps based on their rating. Apple’s rating system includes four categories: 4+, 9+, 12+, and 17+. See Apple iTunes Store and product descriptions as of June 26, 2010.

tent management tools for parents.<sup>11</sup> As the *OSTWG Report* found, the marketplace for parental controls is functioning fairly well, but more can be done to improve awareness and usage of existing tools while also striving to improve the tools themselves.<sup>12</sup>

In addition to the *Guidelines for Carrier Content Classification and Internet Access*, CTIA has worked with carriers and other members of the wireless ecosystem to extend this successful, self-regulatory model to location based services (“LBS”), common short codes and mobile financial services. With the aggregation of personal information on the Internet and evolving wireless ecosystem which may rely on, use or incorporate the location of a device to provide or enhance a service, great diligence is necessary to safeguard privacy, prevent fraud and unwanted dissemination of personally identifying information (“PII”), especially with regard to children. CTIA’s *Best Practices and Guidelines for Location-Based Services* (“LBS Guidelines”), built on the now familiar foundation of “Notice-and-Consent,” promote and protect user privacy as new LBS services are developed and deployed.<sup>13</sup>

CTIA’s *LBS Guidelines* provide special protections for children, and they recognize that in some circumstances—including protecting the safety of children—a wireless carrier’s account holder (rather than an authorized user, such as a child) may need to determine whether LBS may be used at all or a location disclosed to a third-party. For example, a parent/account holder may want to subscribe to LBS to know when a child arrives at school or may want to prevent the disclosure of a child’s location information for safety reasons. Importantly, CTIA’s *LBS Guidelines* are expansive in scope by applying to *all* LBS providers, including application developers and equipment providers, and not simply limited to wireless carriers. These guidelines, which CTIA recently updated to reflect changes in the technology, the market, and consumers’ demands, are an example of how self-regulation has the flexibility and the speed to adapt to the rapidly evolving wireless ecosystem.

CTIA understands that protecting children in these online and mobile environments is a challenging task for the industry, government and—especially—parents. Despite these challenges, the wireless industry continues to respond with effective, innovative solutions to empower parents with choice and control over the mobile content and services their children increasingly utilize. However, Congress should recognize the consensus of online safety experts and industry that there is no single, one-size-fits-all parental control technology or safeguard for all media platforms because of the great variety in capabilities and operating systems, even among competing providers within the same media platform, and rapidly innovating technologies.<sup>14</sup> As the Working Group recommended, government policies can and should encourage stakeholders to help educate parents and children regarding safe, responsible mobile device practices that are already available.<sup>15</sup>

*b. The Wireless Industry Develops and Implements Educational Outreach and Partnership Efforts to Empower Parents and Educate Children*

Even with the availability of parental control tools and self-regulatory best practices, CTIA recognizes that education and information are the keys to helping parents navigate the diverse marketplace of parental control tools and keep up with their children’s evolving mobile usage. For this reason, CTIA and The Wireless Foundation recently announced *Be Smart. Be Fair. Be Safe: Responsible Wireless Use* (“Be Smart”) ([www.besmartwireless.com](http://www.besmartwireless.com)), a national education campaign focused on equipping parents with the necessary materials and tools to help children use their wireless devices responsibly. This site features resources such as sample family rules for parents, lesson plans for teachers, information about the latest research and surveys, and a toolkit with links to parental controls features offered by our member companies.

Launched in March 2010, the “*Be Smart*” campaign has already reached millions of viewers and listeners of newspapers, magazines and radio stations around the country. Just last month, The Wireless Foundation held a “*Be Smart*” event with Illinois Attorney General Lisa Madigan to bring together local and national online safety experts, parents, law enforcement and industry representatives to discuss the latest research and initiatives in mobile online safety and more events are being

<sup>11</sup> FCC Child Safe Viewing Act Report at ¶104.

<sup>12</sup> OSTWG Report at 60.

<sup>13</sup> In April 2010, CTIA released an update of the wireless industry’s voluntary “Best Practices and Guidelines for Location-Based Services,” which promotes and protects the privacy of wireless customers’ location information. CTIA—The Wireless Association®, Best Practices and Guidelines for Location Based Services, [http://www.ctia.org/business\\_resources/wic/index.cfm/AID/11300](http://www.ctia.org/business_resources/wic/index.cfm/AID/11300) (last visited June 28, 2010).

<sup>14</sup> See FCC Child Safe Viewing Act Report; OSTWG Report at 65.

<sup>15</sup> OSTWG Report at 65–66.

planned. In addition, the “*Be Smart*” site links to CTIA and the National Safety Council’s *On the Road, Off the Phone* campaign to educate young people and empower parents to talk to their teenage drivers about the dangers of potential distracted driving resulting from cell phone use while behind the wheel.<sup>16</sup>

As the *OSTWG Report* recommended, these education and awareness-building efforts are absolutely crucial to ensure parents have the tools they need and children are taught to make informed and responsible choices. In March 2010, CTIA joined representatives from industry, academia and online safety advocates to support Congressional legislation which promotes online safety education through government grants to educational agencies, nonprofit organizations, and schools to carry out Internet safety and digital media literacy measures in schools to prevent harm from occurring in the first place.<sup>17</sup> Grant recipients would be authorized to use the funds to develop tools to teach children how to safely, securely and ethically use the Internet and support peer-driven Internet safety initiatives and develop public education campaigns to promote awareness of online risks and improve the health of young people.

CTIA also supports efforts to coordinate and share information at the Federal and state levels. For example, the recent efforts between the FCC, Federal Trade Commission (“FTC”), and the U.S. Department of Education (as part of the OnGuardOnline public-private coalition) to release the Net Cetera online safety guidebook for parents is a positive example of how government agencies can help protect children. Among other things, the *Net Cetera* guidebook can help parents communicate with their children about using mobile phones safely and responsibly and *OnGuardOnline.gov* provides links to information about available parental control tools and technologies across technological platforms. CTIA also supports efforts of state Attorneys General to provide information and education about issues such as cyberbullying, textual harassment and online predation of children.<sup>18</sup> Given these ongoing public and private initiatives, CTIA believes that awareness and outreach can help parents utilize the available tools and that education is the best way to ensure children are utilizing mobile devices and services for responsible and positive purposes.

### III. Conclusion

Today’s tech-savvy children continue to embrace mobile technologies for educational, entertainment, safety, and other purposes. The wireless industry has proactively deployed effective tools that empower parents, and it will continue to innovate in the future. As the wireless industry develops innovative devices, cutting-edge applications and deploys next-generation networks, CTIA believes that our industry’s best practices must continue to evolve to reflect the growing consumer demands in the wireless ecosystem. It is our hope that the *OSTWG Report* will help to inform online safety initiatives at the Federal, state and local levels of government and further encourage partnerships with the wireless industry to educate parents and children about responsible wireless use. We look forward to working with this committee to craft policies which properly balance the need for flexibility in responding quickly to behavioral, technological and market changes. The Wireless industry believes with voluntary initiatives and strategic collaborations, we will continue to ensure the delivery of the benefits of wireless products and services to all Americans. Thank you.

## ATTACHMENT A

### WIRELESS INDUSTRY INITIATIVES TO EMPOWER PARENTS

#### Parental Empowerment Tools

*Content filters*—Wireless carriers may provide parents with the ability to filter content available on a carrier’s network. Wireless carriers, manufacturers and third party vendors may also offer wireless content filters for open Internet access.

*Calling and text limits*—Wireless carriers offer a variety of calling, text and data plan options which allow parents to place limits on the amount of wireless services their children use.

<sup>16</sup>On the Road, Off the Phone: How to Talk to Your Teenagers, <http://info.howcast.com/onroadoffphone> (last visited June 28, 2010).

<sup>17</sup>See Adolescent Web Awareness Requires Education Act, H.R. 3630, 111th Cong. (2009) (“AWARE Act”); see also, School and Family Education About the Internet Act of 2009, S. 1047 111th Cong. (2009) (“SAFE Internet Act”).

<sup>18</sup>See, National Association of Attorneys General, 2008–2009 Presidential Initiative—Year of the Child: Protecting and Empowering Our Next Generation, <http://www.naag.org/year-of-the-child1.php> (last visited June 27, 2010).

*Camera function limits*—Wireless devices may include password protected locks on camera and video features. Wireless carriers offer data plans which allow parents to place limits on the use of e-mail and picture messaging.

*Parental notifications*—Wireless carriers may offer features to notify a parent when a child sends or receives calls or messages from unknown sources or when their child's wireless device leaves a specified area.

*Pre-approved calls*—Wireless carriers may offer features which allow a child's wireless device to receive or send calls or messages only to specified numbers.

*Purchase limitations*—Wireless carriers offer plans and features which allow parents to place limits on the type of content a child may purchase such as music, games, and video. Wireless devices may also include built-in feature limitations.

*Ratings*—A system for classifying and providing information about specific content such as games, music, video and apps. Wireless carriers and manufacturers may rate content or utilize existing rating systems to help parents filter content for children.

*Time of day restrictions*—Wireless carriers may offer tools to limit wireless usage to certain periods (*i.e.*, non-school hours).

### **Educational Outreach**

*Be Smart. Be Fair. Be Safe. Responsible Wireless Use*—Together with kids, parents, experts and educators, The Wireless Foundation and our member companies, CTIA developed the *Be Smart.* campaign to help parents, educators and policymakers locate and utilize the tools and information necessary to ensure children make the right choices when using their wireless devices and services. The campaign's cornerstone is its website ([www.besmartwireless.com](http://www.besmartwireless.com)) which offers a tool kit of the parental control features and filters that are offered by the CTIA's member companies and an example of family rules; educators are provided two lesson plans for 6th–12th grade students; and policymakers can learn more about industry initiatives as well as suggestions on what they can do to help foster the digital future.

*Get Wise About Wireless*—A partnership between the Wireless Foundation and the Weekly Reader Corporation Consumer & Custom Publishing that equips parents and teachers with tips and tools to help students defeat digital bullies by practicing proper cell phone etiquette and safety behaviors. Educational kits sent to schools contain an educator guide, a family take-home pamphlet, a classroom poster and a student mini-magazine. ([www.wirelessfoundation.org/getwise](http://www.wirelessfoundation.org/getwise))

*On Road, Off Phone*—As teens and novice drivers learn the complex task of driving a motor vehicle, safety should always come first. The wireless industry and National Safety Council urge teens to adopt an “On the Road, Off the Phone” philosophy to avoid the dangers of distracted driving. ([www.onroadoffphone.org](http://www.onroadoffphone.org))

*Wireless Carrier Tools*—Wireless carriers offer websites which highlight their parental empowerment tools and educate their customers about responsible wireless use. ([http://www.besmartwireless.com/pages/tools\\_from\\_the\\_wireless\\_industry](http://www.besmartwireless.com/pages/tools_from_the_wireless_industry))

### **Partnerships**

*National Center for Missing & Exploited Children (NCMEC)*—In 2008, CTIA and our member companies joined forces with NCMEC to keep child pornography off of wireless networks by creating the Wireless Child Safety Task Force, whose mission is to help keep wireless devices and services free of child pornography.

*Family Online Safety Institute*—In 2009, CTIA and FOSI held a joint conference where Federal and state policymakers, industry leaders and online safety advocates discussed major challenges and solutions for children in the mobile environment.

*National Crime Prevention Council*—The Wireless Foundation and NCPC developed the 2009–2010 *Crime Prevention Month Kit: Staying Safe in a High-Tech World*.

*National Safety Council*—The wireless industry and National Safety Council teamed up for the driving “On the Road, Off the Phone” campaign.

Senator PRYOR. Thank you.

Again, I want to thank the panel for your testimony.

And since we have the Chairman of the Commerce Committee here—

Senator Rockefeller?

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

The CHAIRMAN. I'll put my statement in the record, but I'd probably revise it to make it copy what Mr. McIntyre said.

[Laughter.]

[The prepared statement of Senator Rockefeller follows:]

PREPARED STATEMENT OF HON. JOHN D. (JAY) ROCKEFELLER IV,  
U.S. SENATOR FROM WEST VIRGINIA

Thank you, Senator Pryor. And thank you for all of your hard work on this important hearing.

As Chairman of the Consumer Protection Subcommittee, you've been such a strong advocate for protecting kids and teens in our digital world. I appreciate your leadership on this issue.

I know this is a concern weighing heavily on the minds of so many parents across America, and we are both deeply committed to doing all we can to safeguard our Nation's youth.

When most of us think of a "bully," we think of a big kid picking on a smaller kid on the playground, or stealing his lunch at the cafeteria.

In those scenarios, the bullying is confined to a school. There are teachers, principals and parents to turn to.

But the Internet—and our new digital world—has changed things. It has made the ability to bully and harass more pervasive, more anonymous, and, in many ways, more insidious.

Even in the confines of his or her own home, a child can become the victim of vicious e-mails, text messages, viral videos, or the subject of cruel rumors that spread like wildfire.

Very tragically, such cruel behavior has, in some cases, driven some desperate and devastated teens to take their own lives.

Cyberbullying is just one example of the threats our children face in our online world. Unfortunately, there are many more.

The Internet, for all its good—and there really is so much good: rich resources, educational material, networking advances—can also be fraught with violent and sexually explicit sites.

Unfortunately, many parents do not know what their children do online—or cannot comprehend the magnitude of the risks they face.

So the questions we must answer today are:

- What are we going to do about it?
- How do we better protect youths in our online world?
- And what tools can we give parents, teachers and kids to empower and protect themselves and their loved ones?

I don't pretend there's an easy answer, but I do firmly believe we can do better—and can do more—to protect our youth online.

Our efforts will require all of us—parents, the private sector, government and educators—to work together.

But when the challenges we face involve the safety of our kids, we all must get involved.

I believe:

- the private sector must be more proactive in taking steps to safeguard kids' online safety and security.
- State and local governments must raise awareness about the problem—and educate and empower kids about proper and safe online behavior.
- Congress also has a critical role to play. If companies do not act to better address children's online needs, then Congress should.

As long as I am Chairman of this Committee, I will continue to work toward a safer online environment for our kids. Inaction in the face of this growing problem is simply not an option.

Thank you again, Senator Pryor, for holding this very important hearing.

I look forward to hearing from our witnesses today.

Senator PRYOR. Well, let me go ahead and call on you to ask the first questions.

The CHAIRMAN. Well, I got here after you two did.

Senator PRYOR. Now, we—we've already worked it out. We insist. Go.

[Laughter.]

Senator PRYOR. You're the Chairman. Go. It's your turn. Am I going to have to hit you—

The CHAIRMAN. What about—

Senator PRYOR.—with this gavel?

The CHAIRMAN.—ladies first?

[Laughter.]

Senator PRYOR. She's fine with it. She's fine with it, I promise.

Senator KLOBUCHAR. I promise.

Senator PRYOR. You go.

The CHAIRMAN. OK.

Ms. Rich, the argument is made—now, I'm very skeptical on this subject. And I hear Mr. Snowden talk about, "We're doing everything we can. We're sort of staying ahead of the curve. And, oh, by the way, can't we have more government grants to educate the people?" And he sort of implied that they were doing everything they could to educate the people. And so, I guess, logically, he'd be correct—one plus one equals two. But, I think, basically, what they want to do is make money and that the rest of you, and this particular Senator, have a—sort of a different approach to it.

What is the FTC's assessment with regard to teens, 13 through 17? We've agreed that kids under 13 are incapable of making, you know, intelligent—or mature, informed decisions. Does the same hold true for—on this matter, does the same hold true for 13 through 17?

Ms. RICH. We believe there are significant challenges, in terms of the impulsiveness and the judgment of teens, they're not functioning like adults, and they don't have the decision-making capacities of adults to protect themselves. But, in terms of the COPPA model and whether you can impose parental consent for teens' use of technologies and the collection of information for teens, we are very skeptical that that model would work for teens. They have access to the Internet through all sorts of outlets outside the home. They're more likely to alter their age information, in order to get online. They may not readily go to their parents and ask for permission. So, we don't believe that that model would work for teens, but we're happy to work with the Committee to develop appropriate protections for teens, of a different sort.

The CHAIRMAN. Well, I might ask you to explain that. But, let me ask another question. The whole concept—and we've been through this in so many ways, on so many subjects—of parental responsibility, whether it's the use of the remote, blocking out—listing and programming in what programs can and can't be seen. I, unlike, Senator Pryor, who comes from a very large and urban and sophisticated state—I come from a rather small and rural state. And parents really don't have a whole lot of time for that, or a whole lot of instinct for that, or, in many cases, any training at all for that.

I mean, and there's the television set. They know how to turn it on and off, the way they used to work, but the whole concept of the technology of a remote is now extraordinary. I mean, they're so large and long, have so many buttons that you actually have to get very conversant with them, almost talk to them, to find out where the mute button is. Takes—that's probably 15 minutes just to find the mute button. So, expecting parents—yes, we should expect parents to do that, but is that not—maybe I should just ask you: What percentage of parents, roughly, in this country, would you say, are actively and effectively engaged in dealing with their younger children, with respect to the subject of today?

Ms. RICH. I don't have a figure for that, but we are—

The CHAIRMAN. Don't have to. You could guess.

Ms. RICH.—we—I really wouldn't be able to estimate that. But, we are working hard to get our booklet *Net Cetera*, which is all about parents talking to their kids about the use of these technologies, into the schools. Just in the last 10 months, we've distributed 3.7 million of them. One came home in my 12-year-old's backpack, and he gave it to me, and we talked about it. We'd already talked about those things.

The CHAIRMAN. Well, you work for the FTC. I would have hoped you would have talked to him—

Ms. RICH. Right. Yes.

[Laughter.]

Ms. RICH.—and we intend to do that. That being said, I agree that education is not the only solution, because people are busy. There's more that could be done. Mr. Snowden talked about controls on cell phones. I think more could be done to educate parents about those controls, because I think phones provide the unique opportunity to add controls at the outset, because parents still pay for most phones. And, I know, when I got my 12-year-old a cell phone, I was not told about all of the defaults that I could set, and, as a result, we got home, and he was on the Internet and using all sorts of games that I did not think I got with my phone, and was very unhappy about.

In addition, enforcement is hugely important in this area. And the FTC has a long record of enforcement against companies that misused children and teens information. GeoCities, Liberty Financial, Toysmart, Gateway—I could name a lot of cases. And, most recently, we sent a letter to a company that was potentially planning to release very sensitive information about gay youth, the XY Company. So, enforcement is also very important in this area.

The CHAIRMAN. OK. Ms. Rich, my time has run out, but I just—I want to take the concept that this is not just another subject that we're talking about. I think this is a game-changer, in terms of the values that our children will grow up with and carry on. What Mr. McIntyre or Ms. Collins, either one of them, or both of them, said, reading is no longer, sort of, appropriate behavior; thinking is not necessarily appropriate behavior, you have to do some of it at school, but you certainly don't have to do it when you're, you know, doing what we're talking about here, or watching television, you just watch, somebody else thinks for you. And I really—I think it's a huge problem for our culture and for our future, because we are so open and so free and so noninterventionist. People can take ad-

vantage of vulnerability, at great profit, and yet not be tagged with being, themselves, purveyors or encouragers of predatory or bullying or whatever type behavior.

I think we have to think very seriously about whether we can let people continue to think that way. It's not just a matter of educating people what they could do, but it's a matter of scaring the heck out of people about what's going to happen to—what is happening to their kids, that they don't know about.

Thank you, Mr. Chairman.

Senator PRYOR. Thank you.

Senator Wicker.

**STATEMENT OF HON. ROGER F. WICKER,  
U.S. SENATOR FROM MISSISSIPPI**

Senator WICKER. Well, I think I will follow the Chair's lead and insert my statement in the record.

[The prepared statement of Senator Wicker follows:]

PREPARED STATEMENT OF HON. ROGER F. WICKER, U.S. SENATOR FROM MISSISSIPPI

Thank you, Mr. Chairman, for holding this hearing on protecting young Americans in an online world. This is a very important topic, which deserves and requires continuing research and investigation if we are to keep up with the ever-changing Internet. It is also an issue that I know you and I both are interested in personally, and I commend you for your commitment and determination to ensure that our youth are protected online. I look forward to continuing to work with you to find the best way we can assist educators, industry, and most importantly parents in keeping their children safe online.

The Internet is unquestionably one of the marvels of modern times. Accessing the World Wide Web has impacted our daily lives as much as nearly any technological achievement in history. Education, entertainment, travel, commerce and even health care have all been revolutionized by the Internet's influence. Access to online content has gone from a luxury to a virtual necessity in the classroom, boardroom, and even the offices of the Capitol. One of the most critical components to the Internet's success has been its dynamic nature. It is changing and growing constantly, unencumbered by unnecessary regulation and driven to provide a better product that meets increasing consumer demand. However, this continuous evolution also presents one of the Internet's biggest challenges.

Keeping pace with technological changes is a difficulty that many industries face. It seems that almost every day a new service, application or product is unveiled that is a little faster, better, and more complicated than those we were using yesterday. This presents new and unique challenges in efforts to ensure that online technologies are safe for children. We continue to search for the right balance that will ensure safety without unnecessarily restricting development of beneficial products. Finding that balance is especially challenging when we are discussing content viewed and used by people of all ages.

Children today are interacting in new ways online and often are providing the content themselves. Through mobile broadband and texts, many of today's children are connected to each other and the Internet. This fact was underscored in a recent report by the Pew Internet and American Life Project, which found that 72 percent of teens use text messages and almost 60 percent of 12-year-olds own a cell phone.

Gone are the days when the best advice to parents for protecting their children online was to monitor their child's activity by putting the family computer in a visible location in the house. Today, parents must get involved directly and talk with children about what they are doing online and how to do it safely. One problem is that most parents know less about these technologies than their children. We must all work together not only to equip parents with the best tools to keep their children safe but also the knowledge to use the tools effectively and to talk to their kids about safe behavior online.

Industry, child advocacy groups, and relevant government agencies have made great strides studying the online dangers for youth, and in finding ways to protect children. Several of our witnesses participated in the Online Safety and Technology Working Group, which recently published a report titled "Youth Safety on a Living

Internet.” This report acknowledged that there is no one silver bullet answer for keeping children safe online.

I am particularly interested in the report’s finding that there are numerous tools available for parents but more needs to be done to improve awareness and usage of these resources. That is one area I would like to explore further with our witnesses today. Working together, what can we do to help parents better understand the problems they are facing? What tools are available to help them? And how do we encourage parents to utilize these tools?

I want to thank all our witnesses for being with us today and sharing your expertise on this topic.

Senator WICKER. Thank you, to the Chairman of the Subcommittee, particularly for the efficient way in which he has run this hearing today, getting it started as the vote was going, and moving it along at an efficient pace. So, thank you, Mr. Chairman, for your concern with this. And my statement in the record will stand.

I hope it’s still all right for Americans to make money in this industry. Mr. Nigam, I would assume that the people at MySpace don’t mind making a dollar, either. I think there’s a way for innovation and investment and job creation to occur in this industry while still protecting children and young people, and I hope we can do that.

I appreciate the testimony of all of you.

Let me just ask this, and I’ll start down here with Mr. Snowden, and maybe people can respond if they disagree. I’m trying to figure out where we might have differences of approach on the panel.

Mr. Snowden, you say, “We look forward to working with this committee to craft policies which properly balance the need, on the one hand, for flexibility in responding quickly to behavioral, technological, and market changes, with concerns”—and I’m paraphrasing your words—“concerns for safety.” So, what are your specific concerns there, Mr. Snowden, that might upset the balance between the need for flexibility in innovation and safety?

And also, you say, “The wireless industry believes, with voluntary initiatives and strategic collaborations, we’ll continue to ensure delivery of benefits of wireless products and services to all Americans.”

What gives you pause, Mr. Snowden, beyond voluntary initiatives that might have a stifling effect on innovation and keeping the United States on the cutting edge of this industry?

Mr. SNOWDEN. Thank you very much for your question, sir. I think the short answer is: I’m not sure if there is large scale or any disagreement among any of us. We work collaboratively with just about everyone on this panel. And I’ve just met Mr. McIntyre today, but I look forward to working with him as we go forward.

In terms of our concern, is—and I think you saw this in the Working Group’s report—there is no-one-size-fits all. And if you take the mobile space, and you say, “Well, you need to do this,” the—you treat the mobile community the same way you treat the online community, versus e-mail or whatever it might be, or television—it’s not going to work. And I think—we spent a whole year debating this issue of, Is there one way to do this? And at conclusion, as you saw in the Working Group that you saw from Hemu, is that there isn’t one way to do it.

And I think, from our standpoint, we're not in this to make money, in terms of on the backs of exploiting children. That is not our goal. We saw the headlights of what was going on in other industries when we began to watch our industry grow and explode, in terms of the technology. And one of the things that we did immediately, for example, is we started working with the National Center for Missing & Exploited Children on child pornography. We wanted to make sure that wasn't on our networks. We began to work with the FTC. We began to work with other parties so that we could make sure we were smart on these issues, so that we can protect kids.

A lot of this is behavior of children that's facilitated by various products that are out there. We look at it from a three-pronged way that takes education, it takes the law, it takes technology. And so, there is not just one way to do it. It's everything, working together.

Senator WICKER. Anybody wish to take issue with Mr. Snowden in that regard? Follow-ups?

Mr. NIGAM. Yes.

Senator WICKER. Mr. Nigam?

Mr. NIGAM. I noticed you kept looking at me, so I assume that's a hint to say something.

[Laughter.]

Mr. NIGAM. Senator, what I want to point out—I actually want to step back and try to frame the discussion a little bit. And it's partly in response to what you said, but partly in response to what Chairman Rockefeller also said.

When we looked at these issues—and I, for one, have looked at them for many years—one thing that's become very clear is this, and this is the pain point for parents.

And I know, I was asked to let you know that I'm speaking on behalf of myself rather than News Corporation and—during the question session.

Parents are looking at technology and saying, "It's that thing that my kids know, and I know nothing about." And then they're making a jump to a conclusion, which they don't need to make, but they're doing it. And that is, "My kids know that technology. I don't. And therefore, I cannot raise them, when it comes to technology." And, I think what we have to do is help parents understand that, as parents, they still have the right, the power, and the ability to educate their teens and their kids about safety, just like they did from the day their baby was brought home from the hospital. When they did it with the cribs and teaching them. Then they did it with the parks. Then they did it when they sent their 13-year-old to the mall and said, "You're not going to do this. You're going to stick with your group. You're not going to talk to strangers. You're not going to disclose info." Things like that. And what you'll find is, the lessons they've been teaching all along, if they continue to teach that in these new mediums, whatever they are—it doesn't even matter what they are—those lessons apply perfectly well.

And the second thing you find is that teens and kids actually learn them. We often think they don't, but they do. They learn how to look both ways when they cross the street. They learn how to avoid that creepy guy in the mall or tell somebody there's some-

body in the mall that they want to stay away from. They learn those things.

And then, from a purely business perspective, what's really interesting is, oftentimes people have a feeling, "Businesses got to make money, got to make money, got to make money." What's really interesting here, in the safety area particularly, is that in—businesses actually benefit by doing the right thing—tremendously. And they benefit because their reputation is at stake, and nobody wants their reputation to be tied to predators and other misconduct as, "That's the business where you find that." VCs won't invest in businesses like that. Advertisers won't advertise and align their, you know, billion-dollar-supported brands with businesses with reputation issues or criminal issues and things like that.

So, there's actually an incentive, from day one, to focus on Business 101. And that is, you can do the right thing, and you will be doing the right thing for your business. So, from that perspective, I go back to what I've said before in other settings, and that is: Look at this issue from the perspective of, How do you build a town into a city, into a country, into a state, and look at all the different things you do there, and take those same learnings and start applying them in this area, and help people understand that they can actually do that and succeed that way?

Senator PRYOR. Senator Klobuchar.

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

Senator KLOBUCHAR. Thank you very much, Mr. Chairman. And thank you for convening this important hearing.

As a parent of a 15-year-old that just did her birthday invitations by Facebook, I know how technology has changed our children's lives. The Pew Internet in American Life Project documented that 73 percent of American teens now use social networking website, up from 55 percent, 2 years ago. So, I think it's no surprise, with that exponential growth, that we are looking at this and trying to figure out new ways to respond. The same study found that 83 percent of 17-year-olds, and nearly 60 percent of 12-year-olds, own a cell phone.

So, my question, first, is—in fact, just this morning, I sent a letter to Facebook's CEO Mark Zuckerberg, asking about the feasibility of adding a safety button to Facebook pages of kids under the age of 18.

On Monday, Facebook partnered with a child protection agency to create a panic-button application for users in the United Kingdom, but this application is not available in the U.S. There is a Help button on the pages, but it doesn't—you have to go through two clicks to get to any security information. And, in my opinion, a prominent button or link, given some of the numbers that we're seeing in the numbers with predators on the Internet, would make this a sensible way to handle this, for kids who have no idea what they're getting into, often.

How readily available, do you think—and anyone can answer this—if you want to start, Ms. Collins, because the group that they partnered with in the U.K. was similar to your group—how readily available are public safety materials to teenagers online? Do you

think children know and understand the basic risk and threat? As you know, most children don't always report the threats to law enforcement. And how can we better get information to teens and parents? And does this type of thing going on in the U.K. make sense?

Ms. COLLINS. Thank you, Senator. Those are excellent questions.

One of the most important things, in the online world and the various platforms that children and adults are using, is the ability to be able to report incidents that they find disturbing or harmful, possibly illegal, in an easy-to-do-format, an easy-to-do way. Most companies have an Abuse button, some sort of policy and procedure in place, but if it's not easy for the user to do, they're not going to report it. In most cases, as you mentioned, very often they won't report the incident in the first place. So, the availability of a prominent and easy-to-use, easy-to-find Abuse button, Report button is very important.

There have been discussions, amongst the industry and amongst child protection groups, about the importance of really having some sort of—essentially, if you can imagine a “splash” page, because there are many resources that are really necessary for families to be able to access. Certainly, in my world, it's the sexual predation of children by adults and others. But, of course, there are other issues that people encounter on social networking sites, on the Internet, in general, whether it be, you know, potential domestic violence that they are witnessing information on; suicide; bullying; you know, gender identity issues—that there are many qualified and very good entities out there that we need to be able to find some way to be able to easily point parents, children, concerned members of the public—when they see an incident, something they find disturbing, something they want to report, that they can easily access the reputable entities that they would then be able to make a report to. And working across the industry to do such an initiative, I think, would be very important, because we need to make it easy for people to report something if they find it disturbing or harmful.

Senator KLOBUCHAR. So, the easier it—and the more obvious that it's more available, the better it is for those that could be the victims of predators.

Ms. COLLINS. Well, most companies—yes—most companies also have abuse and compliance teams. Most of the large players have compliance teams that also take reports and—because people really do report many different types of abuse, whether it be language, whether it be content, and, of course, predation. And those companies will make reports regarding the sexual predation of children and online child pornography to the National Center for Missing & Exploited Children.

But, to your point, accessibility and ease of use is critical.

Senator KLOBUCHAR. OK. That's why I was focused on that. And we hope we can work with them on this.

One issue that hasn't been discussed is peer-to-peer file sharing and the privacy concerns that arise when kids use these programs. As you know, these programs are popular with children and teenagers because they can download songs and movies to their computer. Oftentimes, however, children will share personal files, such

as family photos, home movies, family documents, and there are many cases of predators using peer-to-peer networks to download pornographic materials and target kids.

Senator Thune and I have recently introduced legislation that attempts to address the problem of inadvertent sharing on file-sharing networks. I did an event at—actually, at Best Buy, with a number of victims, not child victims, but people who had just simply gone home to work on their computer, put all the documents from their employer on there as they were working on it. They didn't know that their kid had one of these peer-to-peer file-sharing programs on the Internet, and suddenly all of their company's private employee data was stolen and where they became victims of identity theft. We had a number of cases like this.

So, if anyone wants to comment on the peer-to-peer issue.

Ms. Rich?

Ms. RICH. Yes, Senator, this is a hugely important area. And if you talk to people who monitor this area, they say that the amount of information—sensitive information flowing over the peer-to-peer networks is enormous. We recently did a sweep and sent warning letters to many dozens of companies whose sensitive information was exposed over the networks, probably for the same reason you were just describing, which is, their employees downloaded it, maybe at home, or their kids did, and then all this sensitive information—tax records, health information, financial records—was exposed.

So, it's a hugely important area. And I know you have been working on a bill, that we support, that provides greater transparency for this, and warnings. And we're very supportive.

Senator KLOBUCHAR. Anyone else want to add anything?

[No response.]

Senator KLOBUCHAR. All right. Thank you very much.

Senator PRYOR. Thank you.

Ms. Rich, let me start with you, if I may. And I have a copy of your *Net Cetera* publication here. And I'm just curious—I don't know, really, how to ask this, other than say, kind of, on a scale of 1 to 10, how successful do you think this effort has been? And I guess, also, what kind of feedback are you hearing from people on it?

Ms. RICH. Well, it's interesting you should use that number, because we actually do have an online survey we use for our "OnGuard Online," of which this is part, and have asked consumers, or users, to rate it on a scale of, well, 1 to 100. And it's at 79 percent, which is higher than the information provided on other government websites. If you take into account the reach we've obtained through this, I think we're very pleased with where we are. As I said earlier, in less than 10 months, we distributed over 3.7 million. And when one school district finds out another one has distributed it, they call us up and ask for it. So, every week, we take a tabulation, and it rises. So, we're very pleased with how it's going, and we intend to find additional outlets to distribute it.

Senator PRYOR. Great.

Mr. Nigam, let me ask you, if I may, about the children who are online and—you may not be qualified to give, like, a psychological profile, but what kind of—you know, what—is there a pattern out

there about who does the bullying and who gets bullied the most? Or is it just kind of a random selection of kids?

Mr. NIGAM. Chairman Pryor, I have four children, so I can probably create psychological profiles of children.

[Laughter.]

Senator PRYOR. I understand.

Mr. NIGAM. But, that said, in particular, what the research has—and this is research done in four different, I think, specialists doing research, and they all came to the same conclusion, which is really an eye opener, and that is, kids who are at risk in the physical world are the exact same kids who are at risk online. Those who engage in bullying activity in the physical world are the same ones who will engage in bullying activity online. Those who get bullied in the physical world will also be the ones who will get bullied online.

And what this has done is, in essence, confirmed that the physical and the online have really become one. And, I think, as long as we're focused on treating them separately and finding separate solutions, we're actually missing an opportunity, and that is to really look at it from that larger 50,000-foot context and say, "Is there more that needs to be done in the physical side?" And, if it's going to be done, apply that, and make sure it gets applied online. If you find a kid who's bullied or a child, in the physical side, then start engaging and saying, "That could also be happening online"; and vice versa on the bully, which is, if they're doing it in the bully—if your school is saying your child is causing trouble, or another parent is saying that, well, then also start considering, "Are they doing that and extending it to the online environment?" because, more than likely, that's going to be true.

Senator PRYOR. OK. Let me ask you a different question, and that is—you mentioned, in your statement, that MySpace provides to parents and teens and school officials some sort of guide. Is it a written guide?

Mr. NIGAM. Yes.

Senator PRYOR. And wouldn't it be more effective, and perhaps the most effective, if there was something very clear at the point of use, you know, there on MySpace itself, online, that the kids and the parents somehow could utilize. And—or do you already do that?

Mr. NIGAM. Actually, Senator, we have a section on *myspace.com/safety* that is designed specifically for parents, for—and another section for teens, and one for educators—

Senator PRYOR. But—

Mr. NIGAM.—that has the guides for downloading. And on every page, including the front page of the site, there is a Safety button that takes you—

Senator PRYOR. OK.

Mr. NIGAM.—to all the right places.

Senator PRYOR. That's really was what I was asking, because—

Mr. NIGAM. Right.

Senator PRYOR.—I know a lot of companies are well-intentioned, but you've got to click and follow certain links to get where you need to be. And what you're saying, on MySpace, it is there on every page, so they can easily get to it if they need to.

Mr. NIGAM. Right. And this ties exactly back to—from a purely business perspective, it builds reputation with your user base, it builds trust, it's good for business, it's the right thing to do. And that's a good example of why you should do that, whatever business you are.

Senator PRYOR. OK. Great.

Ms. Collins, let me switch to you, if I may, and that is, What are your recommendations on how to generate more awareness about safety resources that are already available to parents and children? I mean, my experience is, most parents really don't have a real good idea that some of these resources are available. So, how do you think we can best get that word out in the most effective way?

Ms. COLLINS. I think it's an excellent question. And, you know, I've participated and gone out to some schools in the evenings or on weekends to do parent events, to talk about Internet safety. And, unfortunately, you usually get the same parents who are probably pretty engaged in their children's lives at that time also.

There are many, many good resources out there for parents, including NetSmartz411, which explains technology in very easy-to-understand language. But, we—you know, all of us, everyone continues to put parents right there at the front line in order to educate their children, but they don't necessarily have the tools of what they need to educate them on.

I think that, just off the top of my head, one of the interesting ways that—maybe would be, rather than expecting the parents to be coming into the schools in the evenings or on the weekends and so forth, bring it into the workplaces. Bring in some of the information, bring it to them, rather than expect them to come to an event at the schools.

I think the schools still, though, are front-line for getting information home to the families. And I agree with much of what Mr. Nigam was saying about making sure that we teach these overarching lessons of safety, rather than teaching to a specific technology, because the one guarantee we have is, it's going to be different in 2 years.

Senator PRYOR. What is the—from your standpoint, Ms. Collins, what's the most alarming trend that you're seeing, in terms of, you know, children being targeted or, you know, just prevalent problems on the Internet with kids? What's the most alarming trend that you're seeing?

Ms. COLLINS. The trend that we're seeing most, just in the last year and a half, 2 years, are the teens creating sexually explicit material of themselves and sending it to others online. We have many cases, and you can pretty much speak with law enforcement across the country working these cases. And they're challenged with these cases, not only on how to respond as a law enforcement officer, but how to intervene with the families. Kids who are producing very sexually explicit materials, sending it to their boyfriends/girlfriends, posting it up on their social networking pages, many of them, you know, the distribution may occur within a small group of their friends or their school, but we've heard from so many kids and teens, the humiliation the long-term impact of it.

And, in fact, there are more cases that we're hearing about, across the country, where a child may put something explicit of

themselves somewhere online, I take it down, send it around the Internet, and someone then can use that to blackmail the child. And we're seeing those cases, really, across the country and around the world. And the hard part then is, When is the child going to be able to tell somebody and report it?

So, I think, right now, the most obvious trend for us is the kids who are using this technology now, lots of technology, lots of privacy, they're at a sexually curious age, and making some poor decisions.

Senator PRYOR. Right.

Well, listen. I'm going to call on Chairman Rockefeller, and he's actually going to take over chairing the hearing for me.

So, thank you very much for your time.

The CHAIRMAN [presiding]. For a price.

Senator PRYOR. Yes, I understand.

[Laughter.]

The CHAIRMAN. It's a busy time here.

The—Mr. Snowden, do you think that—one of the things we've done here in the Commerce Committee is to say that you cannot text or cannot use a cell phone while you're driving. And—

Mr. SNOWDEN. And we support that.

The CHAIRMAN. That wasn't my question.

Mr. SNOWDEN. OK.

[Laughter.]

The CHAIRMAN. The—do you think that—you see, it keeps on growing. People, they may know that it's a—it has nothing to do with bullying or exploitation, but it's just endangerment of other people, including the other person in the car that you're driving or the car that you hit. Five thousand people a year, maybe more than that, die; and I think there's something like—I think it's something like 50,000 a year are wounded, maimed, or whatever, as a result of that behavior.

Now, in this committee, we've sort of agreed that that should be illegal. In other words, the government is intervening in a behavioral matter, having nothing to do with kids, you know, up to the age of 17, by definition, but people much more mature than that who are doing something which is lethal. And so, we would have the choice, I suppose, of saying, "Well, in time, this is going to be apparent." And to which my answer is, "No, it wouldn't be apparent. People just keep on dying, because texting is—you know, is just necessary to so many people." And so, the government has to intervene.

Now, why do you think it is that the government has to intervene in a mature situation leading to a bad or lethal result, in many cases, and many, many very close misses—why is it that the government has to intervene, probably, in that? And, you say—I didn't ask you, but you said you were in support of that. And that's not—that has the same sort of parallel logic involved in it as the subject that we're talking about, which, in fact, worries me much more, for the long-term health of the country.

Mr. SNOWDEN. If I'm following you correctly, sir, the—where we support is—and we've put, as you put it earlier, money behind it by doing a PSA on driving, "On The Road, Off The"—"On The Phone, Off The Road Campaign" about text messaging. We don't

want people doing that. And what states have done around the country is made the behavior illegal. And I think what we're seeing here in this context of what young people are doing is—the question that you're asking me is, Should that be illegal?

The CHAIRMAN. No. I'm saying don't you think it was appropriate—it's appropriate for the government to have to intervene and make it illegal, with penalties?

Mr. SNOWDEN. It depends what you mean by—what the government's saying is—

The CHAIRMAN. If you're—

Mr. SNOWDEN.—illegal.

The CHAIRMAN.—caught texting or using a cell phone in a car.

Mr. SNOWDEN. And we—we've—I have, personally, written letters to—

The CHAIRMAN. So, what's the—

Mr. SNOWDEN.—in—

The CHAIRMAN.—difference?

Mr. SNOWDEN.—support of this in—

The CHAIRMAN. What's the difference? That's the lesser evil than what we're talking about at this hearing, to me.

Mr. SNOWDEN. What is the difference—

The CHAIRMAN. What we're talking about—

Mr. SNOWDEN.—between—

The CHAIRMAN.—at this hearing shapes the future of the way children grow up to be adults.

Mr. SNOWDEN. What I'm not following, sir, is—you're saying—

The CHAIRMAN. Well, I'll try somebody else, then.

Mr. SNOWDEN. Well—

The CHAIRMAN. Ms. Rich, maybe you can respond.

Ms. RICH. Well, can I translate for him?

[Laughter.]

Ms. RICH. What he's saying is that—

The CHAIRMAN. No, no. I don't ask you to translate me—

Ms. RICH. Yes.

The CHAIRMAN.—to him. I asked you to—

Ms. RICH. You want me to answer it?

The CHAIRMAN.—answer my question.

Ms. RICH. You're saying these consequences are even far more serious than the texting—

The CHAIRMAN. For the long-term, I think.

Ms. RICH.—because we're shaping the minds of youth—

The CHAIRMAN. Yes.

Ms. RICH.—and the safety of youth.

The CHAIRMAN. Yes.

Ms. RICH. So, we, at the FTC, would agree that the privacy and safety of teens is immensely important, and that's why we've done all the efforts that I described earlier.

Mr. SNOWDEN. And may I go back to this, sir?

The CHAIRMAN. Well, you can try again.

Mr. SNOWDEN. Sure.

The CHAIRMAN. Neither of us are doing very well.

Mr. SNOWDEN. Well, we're not disagreeing with you. We're not disagreeing with anything you're saying. What I was trying to understand before I answered your question clearly was, Are you say-

ing that the behavior that—of sexting should be made illegal, are you saying that the behavior of cyberbullying should be made illegal? And, in that case, particularly cyberbullying, there are cases—that is illegal. I mean, States' attorneys have already—

The CHAIRMAN. Well, I mean, I—I'd take it in a different—

Mr. SNOWDEN.—. So, we support that.

The CHAIRMAN.—direction. I would say—and, you know, I'm pretty hardcore on all of this. I don't have a whole lot of tolerance. I mean, when the good Senator from Mississippi said—turned the hearing from something about, "Are we getting in the way of innovation in technology?"—not seeming to understand that this is about sexual predating and bullying and all kinds of things. And people—I mean, I—you know, the Internet, to me, is very interesting.

There's nobody here, so I can just talk as long as I want. The—  
[Laughter.]

The CHAIRMAN. It's very interesting. The Internet was a magnificent discovery. Everybody lives and dies by it. At the very same time that we're spending a great deal of time on this committee and on the Intelligence Committee, in which I also serve, working on something called Cybersecurity.

Mr. SNOWDEN. Right.

The CHAIRMAN. Cybersecurity has everything to do with the destruction—the physical destruction or shutdown of the a nation, or large sectors of a nation, at will, by a 14-year-old kid in Indonesia or a state—a hostile state in some other part of the world, so that the Internet there becomes, in fact, both President Bush's, the last one, and Obama's Director of National Intelligence have identified cybersecurity as the national—the major national security threat, more than plutonium, more than dirty bombs, more than all kinds of other things. So, that's one iteration of the Internet.

Then we come to what we're discussing today. So, you know, "We should do more—get out more of these pamphlets," I don't disagree with. But, I want to hear out of your words, the folks who produce this—not produce it, but who produce the instruments that allow it, is a more aggressive attitude about intervention. Now, I don't think you can—you can't monitor what kids are doing, but there has to be—

Mr. SNOWDEN. Correct.

The CHAIRMAN.—some hookup—and maybe, Mr. McIntyre and Ms. Collins, you could help me on this—where people are—they pay a penalty. I mean, surely, if they are turned in or it could be verified, that their cell phone is shut down for a week—I'm talking about something which sort of says, "Uh, this is important. This is not acceptable." And I don't know exactly what it is.

But, just—you know, I can remember when Jack Watson was President of the Motion Picture Association. They were—and I was furious about motion picture indecency and violence and all the rest of it, and the way it's going. And he kept talking about a \$500-million TV—national TV advertising program which he was going to do. And I was on this committee at the time, and so, he brought this magnificent work into reality and showed it to this committee. I didn't want to watch it, because I thought it was such a fraud, that they were, sort of, buying their way out by buying—putting

down X hundreds of millions of dollars, out of their trillions, for national advertising on “Don’t be sexual,” “Don’t be violent,” “Don’t be explicit.” And there’s some evidence to show that, in the war against drunk driving, it had—other effects of that sort had some effect emanating from the government, not from the industry trying to protect its own future. But—and then he wanted to come show it to me in my office, and I wouldn’t see it.

It was not a serious attempt on the part of the movie industry, in that case, to monitor its own content. I could say the same thing to the cable companies. They do not seriously monitor their content. They say, “We do what the watchers want. We give them what they want.” That is ridiculous. They give them what they teach their watchers to want to want. That’s not Shakespeare, but it’s very clear to me.

[Laughter.]

The CHAIRMAN. And that’s the way this world works. That’s the way money speaks. That’s what Wall Street does. That’s what people who have do to people who don’t have. Now, that’s a little bit broad, but you understand. I’m very angry and passionate on this issue.

So, I look at you and I think, “Well, we’re doing the best we can to try, and we’re putting out little pamphlets, or we’re putting out—sending stuff to schools,” all of which sounds to me wholly inadequate when you’re dealing with teenage basic, you know, sexual instincts, bullying instincts, “I’ve got to be stronger than the next fellow.” Did you see the movie “Doubt”?

Mr. SNOWDEN. I did.

The CHAIRMAN. Did you remember the African-American boy who was bullied because he was African American? That made a profound impact on me. He was totally helpless. And it took a Priest to come pick up his stuff that was dumped on the floor. He was bullied.

I cannot tolerate that kind of thing in the world that I want my children to live in. And so, maybe I’ll just address to the panel, so I can just stop talking, What is the best approach to this? A serious, aggressive approach.

We have an Intelligence Committee, and we have an intelligence community, which assumes bad behavior, well proven throughout all of the centuries, from one country to another, or countries within countries to that country, as we now have, you know, cells that are made up of Americans trying to damage their own country’s government. And then we have a military. And the Intelligence Committee informs the military, in case it gets to that stage. We don’t take chances on things that are a matter of national security.

In this case, I’m saying the future of what goes on in the minds, or does not go on in the minds, of our children—our young children—is a matter of enormous importance, if not national security, you know, currently defined.

I—to me, it’s a terribly important matter, and I think your answer to it is within the classic bounds of a sense of corporate responsibility. You want to do the right thing—

Mr. SNOWDEN. Correct.

The CHAIRMAN.—but it just never ends up being effective enough, quick enough. And I don’t think we have a whole lot of

time. And, actually, I don't want you to answer this. I want Mr. McIntyre—I just pick on you, Mr. Snowden, and I get my answers from the others.

Ms. Collins, Mr. McIntyre, could you give me some help on this? And I do it—I mean, I do it—

Mr. SNOWDEN. I'd like to offer some, as well, sir.

The CHAIRMAN. And you will have a chance.

Mr. SNOWDEN. OK.

Mr. MCINTYRE. Thank you, Senator. It's hard to know where to pick a starting point on this, because there are so many different places we could make an impact.

I wholeheartedly agree, from my experience in working with Mr. Valenti and the television industry on the efforts that we've experienced there, and that we continue to experience. I sit on the Oversight Monitoring Board for the Television Rating System, which is mostly just concerned with coming up with a better PSA. And it makes no impact at all. That group hasn't even met since 2008, and we've experienced a lot of difficulties in trying to move that aspect of media forward.

If I may offer, it seems to me that, when we talk about these issues, we tend to still focus on mostly a market-based approach to this. There's nothing wrong with that, but I think it is short-sighted to only have a market-based approach to this. As I have said repeatedly, media, for us, in the Children's Media Policy Coalition and the groups we represent, is a kids' health issue. The exposure to media impacts children's behavior regarding their health. It impacts their physical health, their sexual health, their mental health. It is the most dominant environment they're in, right now, that it—that impacts their health.

The CHAIRMAN. And you're including the Internet—

Mr. MCINTYRE. Yes. Absolutely.

The CHAIRMAN.—and cell phones among those.

Mr. MCINTYRE. Absolutely. All media in this.

If you look at trying to impact health behavior using a market-based approach—and I'm not antimarket when I'm saying this—but, just from a more objective analytical perspective, a market-based approach tends to be reactive. Something happens, then the market reacts around it, and you get this kind of slow trickle effect when that occurs. That's totally inadequate when it comes to a health-based effect, especially for children, which are not small adults. They're different, and they're different, developmentally, well into their teen years.

What is most successful in health-based communities is a prevention approach. You know, we don't want to wait for the disease to happen, and then have to continue to treat it. We really haven't done much there.

And so, it's a real struggle to try to get the media environment involved in that. Yes, it takes all of these great programs that these individuals have talked about to be able have. We need pamphlets. We need education. We need the PSAs. But, it is—I think I could best say, it's, at best, a good half-step. There has to be other things.

We need—most of the agreements on privacy right now are opt-out agreements. We need to be able to have an opt-in agreement,

with informed consent by the people that are participating in that. And “informed consent” is a very specific technical legal term that the health community uses that assumes autonomy and informs in a certain—what’s the other word that I’ve got—assumes a certain ability to be able pursue malpractice, should that be violated.

And so, yes, I think we’ve got lots of other options here, but, you know, when we have another great pamphlet given to us, it really becomes kind of frustrating. We’re not against the pamphlets; we just think it’s a really small half-step to go forward with.

The CHAIRMAN. Ms. Collins?

Ms. COLLINS. Senator, we’re—we review child pornography, sexually explicit images and videos, day in and day out. We’ve received over 140,000—or, I’m sorry, 940,000 CyberTipline reports regarding child sexual exploitation over the last 12 years. The numbers continue to skyrocket. The problem of child pornography, you know, from very, very little children certainly through the teens, you know, with the creating sexually explicit material and so forth.

The type of behavior that we see the teens engaging in, taking these sexually explicit images and videos, they’re modeling it after what they see and what they’re surrounded by. One of the initiatives—it’s a little off point with what you asked, but one of the initiatives that I did want to tell you about, that you may or may not be familiar with—the National Center, during the course of operating the CyberTipline, we come across, every single day, active child pornography websites, that are hosted anywhere in the world, that contain vile, reprehensible images of children being sexually abused or exploited.

We make available, to participating electronic service providers here in the U.S.—those who wish to be engaged, more involved in ensuring that they’re not easily facilitating transmission or access to these types of websites—we make available, every single day, a list of active child pornography Web pages, so they can—basically, provide them the tools that they can do more to try to reduce further proliferation of these images. Many of these children who have been sexually abused, their abusers are long gone and in jail, but their images continue to circulate on the Internet. And industry really can do a lot to try to reduce that.

In addition, we provide industry participating members with hash values, which are basically digital signatures of photographs of child victims of pornography. Some of the—again, some of these children, you know, their abusers are long gone, but their images and their revictimization continues to happen every single day. We provide these tools to the industry, on a voluntary basis, asking them to do what they can to try to reduce the further distribution of these images—not only because it’s the right and legal thing to do, but also because it’s really a victim- rights issue, that something awful happened to a child, and we really should do everything that we can to try to reduce that victimization in the future.

So, we do have initiatives—voluntary initiatives with companies here in the U.S., trying to exchange information. We provide information to other law enforcement agencies overseas, really to try to do—approach it from many different angles. Certainly, law enforcement arrests the people who are abusing our children; try to educate the kids and the parents and the community at large about,

“These are the things you need to watch for. If something happens, please report it”; and, finally, working with the industry, trying to give tools, also, that they will be able to do more, really trying impact it from many different levels.

Ms. RICH. Mr.—

Mr. SNOWDEN. Mr. Chairman, may I—

Ms. RICH. We’re all—

Mr. SNOWDEN.—may I address it, as well—

The CHAIRMAN. Yes.

Mr. SNOWDEN.—sir?

The CHAIRMAN. Yes, you can, in a minute. Two things on my mind.

I have held so many roundtable or, you know, classroom discussions with superintendents and parents and psychologists and teachers and students all over West Virginia. I mean, this is a very, very big subject, as far as I’m concerned. And I really have the feeling that those meetings, when you put them all together, have made virtually no difference at all. Because the parents who came were the ones who—you know, the—we asked parents, or we asked the school to pick parents. And so, maybe they picked, you know, the most with-it, tech-savvy parents, or maybe they pick really good parents. But, I think the—my impression is that most of the parents of most of the kids don’t show up at those things because they—they’re scared to, because they would show that they didn’t know how to do the remote-control stuff, much less how do you intervene in—you know, in something which goes up on a blog, or whatever. And, you know, on blogs, you can take things down. You can take things down.

So, can you just discuss—and then I’ll get to you, Mr. Snowden—can you—any of you discuss the taking down—and somebody, a moment ago, suggested liability, suing. Boy, that’s a stopper. That’s a national attention-getter, too. Now, I don’t know—would you—you wouldn’t it on the kid, I think you’d do it on the ISP. I mean, I don’t know. What—how can you take stuff down so that the kid who sent it is embarrassed, maybe becomes a little local news story? I mean, I don’t know. What—I—but, I know you can take stuff down. Who can do that?

Ms. COLLINS. Whoever owns the servers can do that. And bringing it to the attention of whoever owns that server, whether it’s an online service provider, whether it’s an Internet service provider—bringing that to the company is the first step. Then, of course, reporting it. Somebody needs to know to be able to take it down. You know, most members of the public and most parents, you know, if there’s something very disturbing up there about their child—inappropriate photos, whatever it may be—would not necessarily know how to contact a company to try to take those steps.

The CHAIRMAN. Right.

Ms. COLLINS. Many companies do, in fact—certainly, with child pornography, there is really no problem with getting companies to take that down. It’s illegal material, and it’s violations of terms of service, it’s contraband.

The CHAIRMAN. Who tries to get it down? Who takes it down?

Ms. COLLINS. The actual company that is hosting the servers. Where the content is—

The CHAIRMAN. So, they do it themselves.

Ms. COLLINS. They will take it down if they're notified, if they become aware of it. Most companies, we have not experienced any problem with them removing that material and reporting it to law enforcement.

Regarding, you know, abusive, disturbing, harassing, upsetting quotes to a blog or social networking site, the different companies would have different policies, I assume. So, I would probably pass off to one of them to determine at what level would they be willing to take it down if a member of the public approached them.

Mr. NIGAM. Mr. Chairman, can I speak from my experience in MySpace and having built the program there?

One of the things that all companies can do is be proactive when it comes to the kind of content that goes on the site. And by that, my—what I mean by that is, employ individuals who actually review the images that are posted, identify ones that have child pornography, hate speech, extreme violence, drugs, paraphernalia, things like that, and remove those and then punish the member who violated the rules.

Second—that's the proactive side—in case you miss something, give every user the opportunity to report an abusive situation in the place where it may happen. In other words, if there's any ability to generate content by a user, that location should also have a reporting capability to allow anybody who's there to let us know.

And then employ the 24/7 staff that actually looks at the reports coming in, prioritizes based on, "Is it suicide?"—goes to the top; "Is it child exploitation?"—goes to the top. And there are lots of—

The CHAIRMAN. You—

Mr. NIGAM.—key words that can be used.

The CHAIRMAN. You mean if somebody takes the initiative—a citizen makes the initiative to report to you, for example, that you will act.

Mr. NIGAM. Absolutely.

The CHAIRMAN. And my question would be—that's a pretty scary thing for a citizen to do. How do they know what they're getting into?

Mr. NIGAM. Well, that's where—

The CHAIRMAN. In other words, my question is, Why wouldn't you set up your own standards for Facebook and what you will allow to appear or what you will—you know, I don't know the answer to it. I'm asking.

Mr. NIGAM. I can answer that. Every company has a "terms of use" that sets the rules and it also sets the expectation of what it allows and doesn't allow. At MySpace specifically—

The CHAIRMAN. But, that's the small-print thing that people get?

Mr. NIGAM. Well, actually, that's the thing that you have to agree to that says, "You are not allowed to post pornography, you're not allowed to harass another member, bully another member, you're not allowed"—and it goes through a list of things. Then the company, like MySpace, proactively, using—

The CHAIRMAN. Yes. But, where do they see that? Where do they get that? How many times do they get that? Does the child or the parent, or whatever—

Mr. NIGAM. Well—

The CHAIRMAN. How many times do you make that—

Mr. NIGAM. Children actually get the message more, because, when they are signed up, they get special messages that are different than what adults get. But, at the bottom of every page, the terms are—if you click on it, in front of you will pop the terms. And that's every page you're on, this site.

But, I think the more important focus point here is, How proactive is a company in enforcing the rules? In other words, is it using keyword technology, like MySpace does, to trigger a review that, because there may be something bad in this area, "Staffer go and take a look at it." And if there is something bad remove it, report it to law enforcement if it's illegal, punish the user, take action. And then follow the trail deeper. If, for example, you're finding an adult who has befriended some kids, and one of them is saying, "I think he's exploiting me in some sense," not only do you act on that, you then look at everything else that adult may be doing, and follow the trail to see if there's a criminal case to be reported to law enforcement.

So, I think companies can be a great deal more proactive than they, historically, have been. And it is—and, Senator, I agree with you on this—it's time to change the paradigm on how companies approach bad behavior, unwanted behavior, illegal behavior, from simply a reactive, "Let me know and I'll take it down," to a proactive, "Let me identify it before the user base does, or before victimization occurs."

Ms. RICH. Mr. Chairman?

The CHAIRMAN. Yes. I've got to do Mr. McIntyre, then Mr. Snowden, and then Ms. Collins.

Mr. MCINTYRE. Thank—

The CHAIRMAN. And then, Ms. Rich, you're—

[Laughter.]

Ms. RICH. If we have time.

The CHAIRMAN.—you have life, as of this afternoon, right? The FTC lives.

Ms. RICH. Right. Terrific.

[Laughter.]

Mr. MCINTYRE. That's good news.

Ms. RICH. Yes.

Mr. MCINTYRE. Thank you. I'll be brief.

It seems to me, when I think of enforcement in this area—I am not a techie, by any means, but my, kind of, an external observation is that these companies are incredibly efficient—even cutting-edge—when it comes to identifying and prosecuting copyright enforcement and trademark infringement. I would wonder if there was something in that process, that those companies employ, that would allow for them to also pursue these other infringements with equal enthusiasm.

The CHAIRMAN. Mr. Snowden, then Ms. Collins, and then Ms. Rich, and then we'll probably wind up.

Mr. SNOWDEN. There are a lot of ideas that have been presented here. And, Mr. Chairman, I would like to say that your passion—you're not alone in that.

And it's not so much the words that I'm conveying on behalf of the industry, I think our actions actually demonstrate this, as well,

particularly as we look at what we've—we embarked upon over 7 years ago. Before we started seeing anything on our networks, we started talking with the National Center for Missing & Exploited Children to make sure child pornography wasn't there. We started working with the various groups. So, it is fair to say that the wireless industry actually looked at lessons from other industries and said, "We want to get ahead of this."

You raised a couple of questions earlier about: Can we just shut the phone down for a week? The question that really gets debated in that is, Who is the—who has the authority to do that? If we were to do that, I would imagine we would be called up here before the Hill, with several different committees and the FCC, because net neutrality rules would probably come into place, about shutting service down and things of that nature. So, we need to look at the competing public policy goals that are going on right now.

We used to have a—for years there was a walled garden that we had in our networks, and we controlled that. Now, with open access, that Congress and other have said, "We want to have more open access, not a walled garden," that means there are less—there's less control. So, there's something that—we need to factor that in as we go through this debate.

I want to convey that we want to work with this committee, and other committees as well, as we go through this, but we have to look at it at a macro level, not just in a micro level of one single public policy goal. From our standpoint—

The CHAIRMAN. No, no. I'm not going to let you get away with that. That—you ended your first statement, that there isn't one single approach to this. And I'm not disinclined to agree—I'm—double negative. I'm inclined to agree with you that there isn't one approach. But, you can't just sort of say that, and therefore, stop, and then saying, "But we were there 7 years ago."

Mr. SNOWDEN. We were there 7 years ago, with our technology, with our industry, figuring out how we can do it for our issues. For example—

The CHAIRMAN. Are you satisfied with what you're doing?

Mr. SNOWDEN. We are very satisfied with—

The CHAIRMAN. You're—

Mr. SNOWDEN.—what we're doing.

The CHAIRMAN.—speaking for—

Mr. SNOWDEN. And we know—

The CHAIRMAN.—a lot of people.

Mr. SNOWDEN.—there is more to be done, because we know, as the evolution—as innovation continues, kids get smarter, technology gets smarter, we all have to get smarter. As you listen to what was going on with MySpace, you put rules in place for MySpace, that may not work in the mobile environment, much like the V-Chip won't work in the mobile or the social networking environment, as well. So, we have to look at it, as the Working Group said, in a macro level and not one-size-fits-all.

The CHAIRMAN. But, don't make it so complicated. Look, that's—it's doable. OK? I mean, you've got—

Mr. SNOWDEN. We agree.

The CHAIRMAN.—you've got, MySpace—I'm sorry, I called you "Facebook," and I apologize.

[Laughter.]

The CHAIRMAN. But, I mean, you've got that, and you've got other venues for it, but there aren't that many. I mean if you have to have a multipronged attack—I mean, when Eisenhower designed Normandy Beach, I don't think he, sort of, said, "Well, we have to do everything the same." He said, "Where are you landing? What are the situations? Where are the Germans planted?"—and all the rest of it. But, it has to be attacked, like we had to do Normandy in order to win that war.

And we have to do something, a lot more than we're doing, in order to win this—or to try to slow down this disease. The great influenza epidemic of 1918. I'm ready to make a comparison. You know, people aren't dying from it, but they're—some are, and their minds are being changed, and they're being turned from readers and thinkers into followers and bullies, and, "I want to please my peers," and all of that. That's been—that was true when I grew up, but we didn't have the tools that are available now. And I think those tools—

It's like the spectrum. Everybody uses the spectrum. And all telecommunications companies think that the spectrum belongs to them. It doesn't. It belongs to the government. It belongs to the American people. And therefore, it can be exercised for the benefit of the American people. Which means that we ought to be—I mean, the FTC—or the FCC, for example, is allowed to comment on promiscuity, but they can't talk on violence. That doesn't make any sense.

In other words, you have to take action at a higher level to cause things to happen at a lower level, I think, unless you don't consider the problem that serious. If it's not that serious a problem, or if the kids are going to evolve out of this behavior because they'll grow up and become more mature and just their—stop their kids from doing it, whatever it is, and then the market works, fine. I don't happen to believe that's going to happen.

Mr. SNOWDEN. Well, that's why we created tools on our networks. We have tools that parents can have by literally just asking, "What are the filtering tools that I can put on my device?" That's why we partnered with the National Center, to make sure we don't have child pornography. And this is why we have launched *BeSmartWireless.com* so that there's—there are tool kits there for teachers and parents and students to understand what the landscape is.

This is a massive issue, and you're absolutely correct. And it's something that I think we have to all work together to try to achieve. And we feel that we are providing the tools, we are working in concert with very—many of these organizations here today, and others, and we want to work with Congress, as well.

The CHAIRMAN. Yes. We always have the choice that, if we don't like what you're doing, we could do something ourselves, right?

Mr. SNOWDEN. Absolutely.

The CHAIRMAN. You don't want that, do you?

Mr. SNOWDEN. Well, we want to make sure that we do something that's balanced.

The CHAIRMAN. I—it wasn't the question I asked.

[Laughter.]

The CHAIRMAN. OK.

Closing thoughts. Anybody.

Ms. RICH. Yes. I just wanted to come back to the issue of consumer privacy, which has been mentioned. You used the term “game-changer” before, and we’re working hard now on privacy issues, because we believe that some of the technologies you’re talking about—mobile social networking, we didn’t mention cloud computing, but all the new ways data is used—are really a game-changer for privacy.

Data is ubiquitous. And right now the dominant model for addressing privacy are these privacy policies which we’ve just talked about. The terms of service, it’s fine print. People don’t stop, in the middle of what they’re doing, to go read the 20-page privacy policy, and then decide, oh, in fact, they’re not going to do what they were doing.

So, we are looking hard—and this is for adults and teens—on whether there are better rules of the road, better ways to manage data collection, because otherwise teens’ data and adults’ data really can be used by anybody.

Mr. NIGAM. Mr. Chairman, first, I want to thank you and the Committee for having this hearing, because one of the things that always inspires solutions is dialogue.

You asked, in many ways, what people were doing, but you’re also, I think, heavily focused on—and this committee is—on what can be done. And I think sometimes, especially in the technology side, it’s hard, when you’re looking from the outside in, to see what the possibilities are, but it’s definitely easier just to ask.

And I think there’s an opportunity here for this committee to convene a series of gatherings, if—perhaps that’s the easiest way to put the word—but, not of the policy folks, like us, but of the engineers, because there are amazingly smart minds in this country who know how to solve problems, using the power of technology. I know the National Center had talked about it, with the image-hashing and the fingerprinting, which I know MySpace uses, and a lot of other companies do. That’s just one tiny example of the power of technology being used for good. There are hundreds of others that can be created. Many are.

But, at some point, I think what we have to do is focus on what to do and how to do, as opposed to what are the issues. It—I think we all know what the issues are, and I think it’s time that we can step forward and say, “Let’s put together the what to do and the how to do.” And the folks who can do the “how to do” are the engineers and that community in this country. And I think this body and others in the government have the opportunity to convene that gathering and convene a series of gatherings like that. And I think a lot of progress can be made through that methodology. OK?

The CHAIRMAN. Mr. McIntyre.

Mr. MCINTYRE. Thank you for allowing closing comments, Senator.

I would say that I’m not sure that we do know what all the issues are here, or that they have been fully acknowledged and realized by the industry representatives. Most of this hearing deals with the critical issues around sexual and child predators. But, ultimately, the heart of the issue is about children and their giving

out information, whether that be through a picture, or whether it be through their personal information, where privacy concerns can arise, or whether it is in ways that it is solicited inappropriately and then used against them by advertisers, as well.

And so, my concern in this is the public health concern. When I look at this report that was just recently generated, as great as it is in dealing with the very limited issues that it deals with, there are no members from the public health community that were a part of that to be able to represent the broader spectrum of health issues that are important to recognize around our children.

This is a health issue for our children. It is a basic health issue for our children. And we would love to see more involvement from the public health community and more involvement of the public health priorities as we go forward on this.

The CHAIRMAN. Ms. Collins?

Ms. COLLINS. Mr. Chairman, it's interesting, when we're discussing future steps—and it is very difficult because there isn't a whole lot of very current research regarding exactly what is happening online, because the platforms keep changing, technology keeps changing quickly, and kids and the Internet are moving fast.

I think that it's very important when—you know, to do timely research, empirically-based findings, in order to determine where exactly to move forward with education, as well as bringing law enforcement to the table. Because law enforcement across the country are overwhelmed with these types of cases, and they're seeing all sorts of things that may or may not come through when interviewing children.

You—the research is needed. We have over 900,000 anecdotes within the CyberTipline. One of my light-bulb moments, you know, over the past few years, working with some of the technologists that Mr. Nigam mentioned—you have these brilliant geniuses who are building all these amazing games and technologies and so forth, and they're creative and they're building these wonderful products that are going to go out there. They're not thinking, for a second, about how those products are going to be used and exploited to victimize children. And in my experience, working with them and talking with them and telling them some of these anecdotes, telling them some of these stories, it helps them really have a light-bulb moment themselves to try to build the architecture of that system a little bit differently so it's less easy to exploit kids, less easy for them—for individuals to take advantage of the system.

I think that really clear examples and cases that would help demonstrate how products will be exploited, potentially, is very important. So, you know, that's a—you know, kind of a forward-movement thing.

But, I think, lessons learned from the companies that have been doing this for some time, so new companies, new products, new platforms may avoid some of the pitfalls that have been seen in the past.

The CHAIRMAN. OK.

Mr. Snowden?

Mr. SNOWDEN. Mr. Chairman, we look forward to working with you and—specifically—and this committee, generally—on ensuring

that consumers have choice and control over their products and services, particularly when it comes to wireless. And I just wanted to say, thank you for the opportunity to be here. We appreciate it.

The CHAIRMAN. OK.

Am I satisfied? No.

[Laughter.]

The CHAIRMAN. But, am I grateful? Yes, to all of you, for coming.

And I'm just very much thinking about when a government and a private sector of enormous power, stand and watch, and sometimes intervene, maybe, as the most vulnerable—you know, kids from 5 to 13, 13 to 17, and, frankly, it certainly goes beyond that—are being exploited and are being taught, through peer pressure and the availability of this medium, and the excitement of it, to lose curiosity as I would—and, I would say, to think less. That's why I'll never—I will always read books. I'm not reading a book if I'm reading it on, you know, iPad or whatever. I'm just not doing it. And I just—I think there are certain disciplines that young people have to go through in the training of their minds. Chess is good, for a reason. Teaching kids to play chess is good, for a reason, because, like going to law school, it makes you use your mind. And it takes up time, then you get into competitions, and you go out and you—you know, a whole new life begins.

Here, what we're talking about is the opposite, and that is—and I will always come back to fine print, because this committee has done so much work on consumer protection, where fine print is the way that people—health insurance companies, pop-up Internet things—you know, come to win over people, because nobody wants to read fine print, and then—well, in the middle of the fine print, there's just a big blue thing saying “Yes” if you want the service. And obviously you think, “yes,” and you don't have to pay for it, you think, and whatever. So, I—the fine print, I think, is a—it was probably a subject for a hearing, but certainly not today.

Something has to happen on this. And I think people on this committee, at least I would think the majority of them, feel pretty strongly about it. And, you know, so we will see what happens.

And I thank you all very much for your courtesy and your time in being here.

[Whereupon, at 4:16 p.m., the hearing was adjourned.]



## A P P E N D I X

AMERICAN CIVIL LIBERTIES UNION—WASHINGTON LEGISLATIVE OFFICE  
*Washington, DC, July 15, 2010*

Chairman MARK PRYOR,  
Subcommittee on Consumer Protection,  
Product Safety, and Insurance,  
U.S. Senate,  
Washington, DC.

Ranking Member ROGER WICKER,  
Subcommittee on Consumer Protection,  
Product Safety, and Insurance,  
U.S. Senate,  
Washington, DC.

Re: Subcommittee hearing on “Protecting Youths in an Online World”

Dear Chairman Pryor, Ranking Member Wicker, and Members of the Subcommittee:

Thank you for offering the American Civil Liberties Union (ACLU) the opportunity to submit this statement for the record in connection with the Subcommittee’s hearing titled “Protecting Youths in an Online World.” The ACLU is a non-partisan organization with more than a half million members, countless additional activists and supporters, and 53 affiliates nationwide. While recognizing the concern many Americans have about the dangers facing children on the Internet, we urge the Subcommittee to avoid taking steps that would criminalize protected first amendment speech and, instead, to support programs that would educate and inform children, parents and educators about online risk prevention and Internet safety practices.

The Internet presents new ways for young people to communicate—but it does not inherently increase the dangers that have been present in human society for centuries. Reported incidents involving youths online have produced heartbreaking stories with which all Americans sympathize. From these reports, one might conclude that the online world is becoming an increasingly dangerous place for children. But it is also well-documented that online activity, particularly among youth, is increasing exponentially and so it is only logical that online incidents—such as online harassment, bullying or worse—would also be increasing. We must not let the compelling nature of these anecdotal reports stand in for a more reasoned assessment of the threats facing young people online.

It is understandable to want to protect young people online. But before taking action in a way that would narrow the rights of adults and youth online, there should be a clear understanding of the differences between online threats and the kinds of issues young people have been dealing with for generations. There is evidence to suggest that some of the reported risks young people face online may be exaggerated. For example, one respected social media researcher at Harvard said that child abduction by a stranger is an extremely rare threat—12 out of 300,000 in a year.<sup>1</sup> It stands to reason that such abductions resulting from online activity are similarly rare. And despite dire warnings that 20 percent of children have been sexually solicited in chat rooms, by instant messenger, or e-mail, it is routinely overlooked that these solicitations overwhelmingly originate with other young people—96 percent—and that such solicitations are easily and typically ignored.<sup>2</sup> The phenomenon of “cyberbullying” has also received attention recently and in a rush to address this problem, lawmakers have forgotten that bullying has been around since long before the Internet. Previously young people harassed and intimidated each other face to face, through third parties, through the mails, by telephone, across the airwaves, and—only now—via Internet communications. Yet there is very little research to suggest the dangers to young people are dramatically worse online than offline. Before taking legislative steps that may restrict online free speech, we urge Congress

<sup>1</sup> Technology Review, “The Moral Panic over Social-Networking Sites” (Aug. 7, 2006) (quoting Danah Boyd).

<sup>2</sup>*Id.*

to make sure it accurately assesses the severity of the threat and narrowly focuses any legislative proposal.

Federal attempts to circumvent the first amendment and regulate online behavior with the goal of protecting youths are nothing new. They began in the mid-1990s with the Communications Decency Act (CDA), which attempted, among other things, to protect minors from harmful material on the Internet by criminalizing the knowing transmission of obscene or indecent messages to any minor recipient or the knowing sending or display of any message that depicts patently offensive activities.<sup>3</sup> After the Supreme Court struck down the CDA, Congress tried again by enacting the Child Online Protection Act (COPA), which provided for civil and criminal penalties for anyone who knowingly posts material that is harmful to minors on the web for commercial purposes.<sup>4</sup> Both laws were declared unconstitutional for overreaching—imposing a broader speech restriction than necessary to achieve the narrow objective of protecting children from obscene material.<sup>5</sup>

Other Federal legislative efforts have been more successful. The Child Online Privacy Protection Act (COPPA) protects children under 13 from the collection of personally identifying information by operators of commercial websites or online services. The Children’s Internet Protection Act (CIPA) mandates that schools and libraries employ software filters to restrict access by minors to inappropriate material as a condition of receiving Federal funds. Many Federal and state legislative initiatives have attempted to impose restrictions, sometimes successfully, on sex offenders in their use of the Internet even after completion of their sentences.

Criminalizing online speech is unconstitutional and will be ineffective. Harassing speech will either continue online in violation of the law or it will simply shift to other spheres within which it simultaneously exists. This does not serve to minimize the potential dangers facing young people online, but rather it demonstrates that we may be better served by working to educate youth on the responsibilities associated with electronic communications.

Legislation has been introduced to inform children, parents, and educators about the risks and opportunities associated with online communications. H.R. 3630 and related bill H.R. 3222, the “Adolescent Web Awareness Requires Education Act (AWARE Act),” offered by Representative Wasserman-Schultz, both have elements aimed at doing so. The latter bill, in particular, would direct grant funds to the development of Internet safety education programs and would provide training and tools to teachers and parents to help keep young people in a position to use the Internet safely. The former bill—H.R. 3630—would put a greater emphasis on crime awareness which in our view misplaces priorities about the Internet, a facility that should be viewed as a vast and expanding resource and not primarily as a place of criminality and intimidation. However, the bill also includes some of the same opportunities for education of children, parents and educators and, as such, represents a better step forward than an overbroad attempt to criminalize certain kinds of online speech.

Young people are always quick to adopt new technologies and this should be recognized and encouraged as we move into the digital age. The Internet has made it easier for them to learn about the world and communicate with others. While some might say that such ease of communication necessitates the need for special restrictions on minors who haven’t learned the restraint that comes with maturity, we believe that any restriction specifically aimed at curbing the speech rights of minors in the new electronic forum is a step in the wrong direction and not in keeping with the ideals of our constitutional framework.

We do not take issue with the Subcommittee’s interest in looking at the issues of harassment, intimidation, or abuse faced by youth, but we would encourage taking a broad view of the phenomenon, not limited to the particular tools of communications used to convey such messages that may lead to harmful actions. For example a review of the tools that the Internet can provide to assist in limiting bullying or harassment, such as documentation of incidents and identifying when intervention is necessary, could yield valuable insights for fighting the problem. If additional legislation at the Federal level is deemed necessary, we would urge the Subcommittee to carefully define its terms before moving forward, taking care to draw any prohibitions very narrowly so as to avoid limitations on protected First Amend-

<sup>3</sup>Telecommunications Act of 1996, Pub. L. 104–104, 110 Stat. 56 (Title V—Communications Decency Act of 1996) (CDA was an add-on to the bill and received no substantial public airing of its provisions, unlike the remainder of the bill).

<sup>4</sup>47 U.S.C. s. 231.

<sup>5</sup>See *Reno v. ACLU*, 521 U.S. 844, 117 S. Ct. 2329 (1997) (CDA facially overbroad); *ACLU v. Mukasey*, 534 F.3d 181 (3d Cir. 2008) (cert. denied) (COPA not narrowly tailored and not the least restrictive alternative).

ment rights. In the meantime, as we still stand on the opening threshold of the Internet age, there is much good that can be done by expanding public awareness of both the benefits and risks associated with online activity and we would encourage the Subcommittee to support such efforts.

If you have questions or comments on ACLU's position on this issue, please feel free to contact Michael Macleod-Ball at 202-675-2309 or by e-mail at [mmacleod@dcacclu.org](mailto:mmacleod@dcacclu.org).

Sincerely,

LAURA W. MURPHY,  
*Director, Washington Legislative Office.*

MICHAEL W. MACLEOD-BALL,  
*Chief Legislative and Policy Counsel.*

---

PREPARED STATEMENT OF YAHOO! INC.

Chairman Pryor, Ranking Member Wicker and members of the Subcommittee, you are to be commended for your continued and long-standing interest in child online safety issues. Yahoo! also has a deep commitment to online safety issues and is grateful for the opportunity to share some relevant information learned through a study we released in honor of National Internet Safety Month in June. Yahoo! was also a participant in the Online Safety and Technology Working Group ("OSTWG") that was set up pursuant to legislation that started in this committee in 2007. In June, the OSTWG issued its report to Congress entitled "Youth Safety on a Living Internet" which addresses several key areas of online safety including education, safety tools, reporting and cooperation with law enforcement. Yahoo! has many activities in these areas and will take this opportunity to briefly describe what is being done in these areas.

**Yahoo! Background**

Yahoo! attracts hundreds of millions of users every month through its innovative technology and engaging content and services, making it one of the most visited Internet destinations and a world-class online media company. Yahoo!'s vision is to be the center of people's online lives by delivering personally relevant, meaningful Internet experiences. Yahoo! is headquartered in Sunnyvale, California.

**Yahoo! Online Safety and Digital Protection Survey**

In April of this year, Yahoo! conducted an online survey with Ipsos OTX to gain insight into consumers' behaviors and perceptions with regard to online safety. The survey is based on a sample size of 2003 Internet users in the United States, ages 18-64 years old. Our goal in conducting the survey was to gain insights into people's behaviors and sentiments regarding online safety so we can better align our safety education, product features, and outreach efforts to user needs. We wanted to drive awareness of National Internet Safety month in June by uncovering trends around online safety—specifically with parents and children and digital reputation management.

The survey interviewed a cross-section of U.S. adults, with 40 percent of the respondents being parents with children of the age of 17 or younger. The survey asked a variety of questions relating to parents and kid's online safety management, including cyberbullying, sexting; and digital reputation management.

The findings of the survey are very encouraging as they show parents are being much more proactive than generally believed when it comes to their children's online safety. The data also shows that there is more work to be done. Overall, Yahoo! gave parents a B+ for their efforts to monitor their children's online activities. Yahoo! also concluded, based on the survey results, that more education and resources are needed to help parents and children address cyberbullying and digital reputation management. More detailed information on the survey findings is attached as a presentation at the end of this document.

**Parents Are Taking Action**

Yahoo! celebrates the parents who are proactively monitoring their children's online safety and are having appropriate discussions with their kids. The Yahoo! survey shows:

- 78 percent of parents are concerned about their children's online safety, with almost 50 percent being "very concerned."
- 70 percent of parents talk to their children about online safety at least 2-3 times a year; 45 percent talk to their children at least once a month.

- 74 percent of parents are connected to their children’s profiles on social networking sites.
- 71 percent of parents have taken at least one action to manage their children’s use of the Internet or cell phones such as:
  - Checking to see where children are searching online.
  - Setting time limits for children’s use of computers or cell phones.
  - Setting parental controls on video sites.
  - Using filters to limit where children go on the web.

This level of parental engagement is an encouraging sign that parents and children are becoming more comfortable with safety issues and discussing them with each other. It also shows parents are embracing the tools that are available to empower them to control their own and their children’s online experiences. But there is always room for improvement.

### **Cyberbullying Findings**

While many parents are actively engaged in their children’s online experiences, cyberbullying presents significant challenges. Most parents are aware of the problems presented by cyberbullying, yet are unsure of appropriate actions to take in response. The data from our survey shows:

- 81 percent of parents know what cyberbullying is.
- 1 in 4 adults (25 percent) who are aware of cyberbullying have either been victims or know someone else affected by cyberbullying.
- 37 percent of parents feel that they know what to do about cyberbullying.
- Almost three-quarters (73 percent) of people want their child’s school to play an active role in teaching kids about online safety and citizenship.

### **Yahoo! Tips on Cyberbullying**

Yahoo! has developed an extensive safety site accessible from nearly every page of *yahoo.com*. Yahoo! Safely (*safely.yahoo.com*) helps inform parents, students, and teachers about online safety through timely videos, simple strategies and advice from non-profit safety experts. Specifically, Yahoo! Safely offers the following tips for young people to help prevent cyberbullying.

- *Own your digital reputation.* The Internet is a public space, so before you share photos or personal details, make sure it’s info that you’d share with teachers, colleges, or job prospects.
- *Keep your private information under your control.* Keeping Internet conversations (and your user names/profiles) free of personal information like your password, full name, or even the name of your school, is important.
- *Be nice (and pass it on)!* Be respectful online and treat people the way you’d want to be treated. If someone is being disrespectful or bullying you, try to ignore them and use privacy tools to block them from viewing your full profile and contacting you.
- *Know your rights.* You have the right to not respond to e-mail or other messages that are inappropriate or make you feel uncomfortable. If you get a message that doesn’t feel right, show it to your parents, guardians, or another trusted adult and report the incident to your Internet service provider.
- *Have a family chat.* Talking with your parents or guardians doesn’t mean giving up your privacy. Everyone benefits when you’re on the same page about online activities, including when you can go online, how long you can stay, and what activities you can do online.

### **Digital Reputation Management Findings**

Digital reputation management is a growing concern for both children and adults as they share more and more personal information online. New stories have reported everyone from potential employers to college admissions officers conducting online searches and considering the findings in evaluating an applicant. The information a user posts online can have important safety consequences, and important long term implications on the user’s reputation.

However, according to the recent Yahoo! online safety survey, 65 percent of people do not know, or are not sure what a digital footprint is and 31 percent do not feel they are in control of their online image. “Digital reputation management” as defined by the study includes both a user’s *digital footprint*—the content and information that is posted by or about a user on the web over time, including online profiles,

comments and blogs—and a user’s *online image*—the way people are perceived based on content.

The survey also concluded that

- 48 percent of respondents do not realize or are not sure if the information they put on the web will remain online forever and 7 percent think that it won’t remain online forever if they simply delete it.
- 20 percent of people plug their own name into a search engine once a month or more; 49 percent do it 2–3 times a year or less.
- Adults ages 18–34 are more proactive about managing their digital profiles than adults 35–49 and adults 50+.

Online safety education has long urged children, and actually users of all ages, to be careful about the types of personal information they post online and who they make it available to—such as information about where they live or where they go to school—as an important part of maintaining their physical safety. Given the many other implications that a user’s online activity can have for their present and future, these survey results suggests that there is a need to cultivate greater awareness among Internet users of all ages about the broader impacts of what they choose to share online.

#### **Yahoo! Tips on Digital Reputation Management**

- *Know your connections:* Only connect with people you know offline.
- *Think before you post:* Once something is posted online, it’s virtually impossible to take back because words, pictures, and videos can be easily forwarded, copied, and taken out of context.
- *Protect your personal information:* Posting personal information or photos can identify you to strangers. Never reveal personal information to people unless you are friends with them offline.
- *Configure your settings:* Take the time to understand the profile settings that are available to you on websites and social networks, and tailor those settings for you.
- *Understand your digital footprint:* On a monthly basis, search for your name on search engines, like Yahoo! Search, and on social networks to understand what type of content is associated with you.

#### **Yahoo! Online Safety Efforts**

At Yahoo!, we are very proud of our long history of promoting safer environments for kids to experience the benefits of the Internet. In 1996, Yahoo! was the first Internet company to launch a child and teacher-friendly web resource of safe, child-appropriate websites. Yahoo! Kids (formerly Yahoo!igans!) is Yahoo!’s award-winning web guide for children ages 7 to 12. All content on Yahoo! Kids has been reviewed by human editors for appropriateness for it’s young audience. Yahoo! Kids ([kids.yahoo.com](http://kids.yahoo.com)) also includes a substantive Parents Guide that covers all manner of media safety, especially online safety issues.

Today, Yahoo! Kids, Yahoo! Shine, and Yahoo! Safely all feature safety information targeted to kids, teens, and adults. Yahoo!igans! was our starting point, but we have grown our safety program into a multi-faceted approach to online safety that focuses on: (1) education; (2) user and ISP reporting; (3) technology and user empowerment tools; and (4) relationships with law enforcement, industry peers and child advocacy organizations. Many of our most recent efforts are directly related to the issues raised in our online safety survey. They also largely coincide with the findings of the recently released Online Safety and Technology Working Group (OSTWG) study entitled “Youth Safety on a Living Internet.”

#### **OSTWG Study and Recommendations**

The National Telecommunications and Information Administration (NTIA) was tasked by the “Protecting Children in the 21st Century Act,” a title of the “Broadband Data Improvement Act,” P.L. 110–385, to create a multi-disciplinary working group to report to Congress on four key areas relating to the safety of children while online. These four areas are: (1) online safety education; (2) parental controls and other empowerment tools; (3) child pornography reporting; and (4) data retention. Yahoo! was pleased to provide expert participation in the OSTWG. The OSTWG issued its report this past June and it included over 30 recommendations for the continued study and improvement of online safety efforts.

As many of the participants in the hearing are likely to comment on the OSTWG report findings, Yahoo! would like to focus on those findings and recommendations that are most relevant to our areas of focus.

### Online Safety Education Findings and Recommendations

The OSTWG Subcommittee on Internet Safety Education made a number of important findings about the elements of successful education and awareness efforts that should be carefully considered by any entity seeking to promote safety education. These findings include that: educational messages should not be fear based nor follow a one-size-fits-all approach given that those who are at risk in the offline world also tend to be at the greatest risk in the online world; messages and advice should be appropriately tailored to the risks being addressed, how technology is actually being used and the intended audience. For example, the OSTWG Report notes that at one point the primary safety advice given to parents was to locate the family computer somewhere central in the house.<sup>1</sup> Today, widespread use of mobile devices makes this messaging far less relevant. Safety education needs to evolve as use of technology evolves. The subcommittee also noted that there are many stakeholders who have key roles to play in promoting safe online practices including schools, parents and online services.<sup>2</sup>

Similar to our survey findings, The OSTWG report finds that cyberbullying is the most serious concern for students, parents, and schools because it is currently the online danger that children and teens are most likely to face.<sup>3</sup>

The OSTWG report offers a number of recommendations that Yahoo! agrees are of key importance to continuing to improve the effectiveness of safety awareness. I would like to specifically highlight a few of these recommendations and the corresponding Yahoo! efforts that support the goals of the recommendations.

- “*Keep Up With Research and Base Education On It*”:<sup>4</sup> Yahoo!’s recent survey, as well as our extensive work with safety experts, is designed to provide the basis for a fact-driven approach to developing on our online safety programs, including which issues to focus on and how best to convey safety messages. We welcome more coordinated national efforts to bring together the great academic and scientific work that has been done in this space and to further develop our common understanding of the risks we want to address.
- “*Coordinate Federal Government Educational Efforts*”:<sup>5</sup> Yahoo! applauds the efforts of government entities, particularly the Federal Trade Commission, for its online safety education efforts. OnGuard Online has been a leading educational effort that, Yahoo!, like many service providers point our users to as a key safety resource both from *safely.yahoo.com* and from *security.yahoo.com*. Other efforts to consider online safety or citizenship funding within reauthorization of the Elementary and Secondary Education Act should also be seriously considered.
- “*Establish Industry Best Practices*”:<sup>6</sup> The OSTWG Report recommends that providers evaluate the specific safety needs of their users and to tailor educational efforts, safety tools and other resources to those needs. In addition, it calls on providers to work collaboratively with other companies, non-profits, schools and governments. Yahoo! has a wide range of programs under way with each of these groups. To name a few:
  - Yahoo! has created educational videos for Yahoo! Profiles, integrates tips and advice into product help pages, and issues regular blog posts to educate people on online safety issues on Yodel Anecdotal (*yodel.yahoo.com*) and the Yahoo! Policy blog (*ypolicyblog.com*).
  - Yahoo! is engaged in partnerships with *Ikeepsafe.org*, Family Online Safety Institute, Teen Angels/wiredsafety, i-Safe, CARU/BBB, *connectsafely.org*, and Commonsense Media. These activists and experts are on the cutting edge of relevant advice, solutions and emerging issues.
  - Yahoo! hosts an annual Cybercitizenship Summit to bring together educational thought leaders to discuss issues, developments, and solutions

<sup>1</sup>*Youth Safety on a Living Internet*, Report of the Online Safety and Technology Working Group, June 2010 <http://www.ntia.doc.gov/reports/2010/OSTWGFinalReport060410.pdf> at 6.

<sup>2</sup>*Id.* at 5.

<sup>3</sup>*Id.* at 12.

<sup>4</sup>*Id.* at 30–31.

<sup>5</sup>*Id.* at 31.

<sup>6</sup>*Id.* at 32.

around youth and online safety. Our last Summit, held on December 4, 2009 focused on cyberbullying and online reputation management.

- Yahoo! has partnered with *Ikeepsafe.org*/DARE to develop Internet safety curriculum for grades K–6. We work collaboratively with *iKeepSafe* in developing the *Project PRO* curriculum, aimed at helping educators coach their students on how to manage their digital reputations.
- Yahoo! increases awareness around online safety throughout the year during Safer Internet Day (February), Internet Safety Month (June), and National Cyber-Security Awareness Month (October). This can include messages on our front page, which attracts over 600 million users per month. Yahoo! has also worked closely with the National Cyber Security Alliance on a consumer messaging project in 2010.
- Yahoo! works collaboratively with local police departments to deliver preventative and diversion safety courses. Yahoo! has been working on a pilot Diversion course with the Sunnyvale, California Police. The course is designed to train students on better online behavior if they receive detention or other sentencing by the courts for online crimes such as sexting.

#### **Parental Control and User Empowerment Tools Findings and Recommendations**

The Parental Control and User Empowerment Tools subcommittee found that the parental control marketplace is functioning fairly well—at least for parents with some degree of technical sophistication—and yet there is more that can be done to increase awareness and usage of existing tools and to continue to improve capabilities. After studying the range of tools in the marketplace—both stand alone solutions and integrated product safety features—and their effectiveness and level of use, the subcommittee developed, among others, the following conclusions and recommendations.

- *User empowerment tools and parental controls are “most effective as part of a ‘layered’ approach to online safety that views them as one of many strategies or solutions.”*<sup>7</sup> In addition, the report found that “technical solutions can supplement, but can never supplant the educational and mentoring role.”<sup>8</sup>
- *“Parental empowerment technologies and options should be included in new offerings whenever possible” and “[s]afety by design” should be encouraged.* The OSTWG also recommends that industry carefully review default settings which are an important element of safety by design. Yahoo! has been examining its default settings in the context of new product and feature launches, and, within the context of the overall operation of the service, attempts to set defaults to embrace safety as a key objective. Examples of “safety by design” and use of default settings include:
  - Enhancements to our social experience within Yahoo! Pulse launched in early June, defaulting users registered as being ages 13–17 to allow only “connections” (those that have been confirmed by the user as a friend) to see their profiles. Yahoo! also has defaulted settings on Pulse for users under age 18 that are designed to steer users away from revealing their ages and addresses.
  - The launch of our “Updates” service where users can post status updates from various places throughout the Yahoo! network also defaults the sharing of these updates to “connections only” for teen users.
  - Flickr, Yahoo!’s photo sharing service, provides various controls for users to tailor their experience including the ability to make photos public, private or viewed by friends and/or family; categorize photos as safe, moderate or restricted content; turn SafeSearch on so only photos designed as safe for a global, public audience will be returned in results; hide photos from public searches; customize settings around privacy and permissions; and the ability to report abuse.
  - The Yahoo! SafeSearch feature is designed to filter out explicit, adult-oriented content from Yahoo! Search results. Yahoo! defaults to a filter that removes adult video and image search results. Parents can password-protect the search filter setting for their computer by “locking” their SafeSearch settings.
  - Yahoo! Messenger allows people to block others from contacting them as well as report suspected spammers and report abuse.

<sup>7</sup>*Id.* at 66.

<sup>8</sup>*Id.* at 7.

- Yahoo! Groups gives users control over how they receive e-mail messages, the ability to block users under the age of 18 from receiving messages, and the ability to report abuse.
- Yahoo! Chat does not support user created chat rooms—all chat rooms are created by Yahoo!; we have restricted usage of the service to 18 and older, no longer support a “teen” category, and have included a “report abuse” button.
- *Community Policing* was also recommended by the OSTWG as an important part of service provider options to allow users to flag inappropriate content and report inappropriate behavior.<sup>9</sup> User and third party reporting have long played an important role in Yahoo!’s safety approach. We use these efforts to help us identify material in violation of our Terms of Service so that we can remove it from our site, discover users who are violating our guidelines, and to assist us in identifying and reporting child pornography content to the National Center for Missing & Exploited Children (“NCMEC”). In addition to leveraging the power of our users to help us identify abuse of our services, we also employ filters, algorithms, human and automated resources to detect child pornography content, as well as work with third parties that have lists of URLs where known child pornography is found.

#### **Child Pornography Reporting Findings and Recommendations**

As a result of the Protect Our Children Act of 2008, Public Law No. 110–401, 122 Stat. 4229 (2008), the reporting obligations for Internet Service Providers, previously captured at 42 U.S.C. § 13032, have been improved by a new law that: (1) clearly states what should be included in a report; (2) provides appropriate immunities for the transmission of images as part of fulfilling the reporting obligation; and (3) provides for preservation of materials included in a report and related to a report.

OSTWG recommendations in this area in large part focus on smaller ISP and OSPs that may not understand or have mechanisms in place to report as required by the new law. Other recommendations focus on the continued need for dialogue with law enforcement and NCMEC, as well as increased technology and information sharing among service providers.<sup>10</sup> Yahoo!’s efforts as a leader on reporting issues is evidenced by our visible presence on these issues over many years.

- Yahoo! features prominent “Report Abuse” links across our network near user generated content to encourage users to flag problem issues.
- Yahoo! was an active participant in developing with industry peers and NCMEC the service provider sound practices for reporting child pornography, which were the model for changes in the law passed as part of the Protect our Children Act in 2008.
- Yahoo! has had a long-time relationship with Internet Watch Foundation and uses the Foundation’s URL list along with NCMEC’s URL list to remove known child pornography sites from its search index.
- Yahoo! is a founding member of the Technology Coalition working to develop improved detection and reporting technologies for child pornography images.

#### **Data Retention in Child Exploitation Investigations Findings and Recommendations**

Unlike other areas of the Report, no clear consensus emerged on whether there is a need for mandatory retention obligations beyond those required as part of the preservation regime in the Protect our Children Act. Instead of attempting to arrive at a consensus view, the Report focuses on conveying the diverse viewpoints of law enforcement, industry, and privacy advocates. Indeed, following the subcommittee’s investigation, there remain many unanswered questions about the need for data retention, the potential scope of data retention, technical costs and limitations, and the impact on user privacy.

- *The recommendation to study the impact of the new preservation provisions of the Protect our Children Act is perhaps the most important.*<sup>11</sup> Yahoo! supported the legislation that became the Protect our Children Act, including the preservation provision, because it was designed to balance law enforcement’s needs for ISPs and OSPs to hold data regarding those who misuse services to exploit children online with the overall privacy interests of the entire user community.

<sup>9</sup>*Id.* at 67.

<sup>10</sup>*Id.* at 89–91.

<sup>11</sup>*Id.* at 116.

This balance was struck by focusing preservation efforts on those users who ISPs and OSPs are already required by law to report as being involved in an apparent incident of child pornography. This focus makes sense because the vast majority of other users will never be investigated for the commission of a crime.

When the legislation was passed in 2008, approximately 30,000 reports by ISPs and OSPs were submitted to NCMEC. However, there were over 60,000 reports in 2009 and over 27,000 just in the first quarter of 2010, on track for a 78 percent year over year increase from 2009.<sup>12</sup> These provider reports provide an important and underutilized means to pursue child predation. This is a well-tailored solution to the need for data retention in online child exploitation cases and should be given a chance to be fully implemented and evaluated on its merits before additional data retention measures are considered.

- *The OSTWG Study further suggests Internet Crimes Against Children Task Forces hold regular meetings with ISPs and OSPs.*<sup>13</sup> This recommendation is in synch with our own online safety principle to work constructively with law enforcement as a partner in creating a safer Internet. That is why Yahoo! has built a law enforcement compliance function to respond to valid law enforcement demands and to be able to respond appropriately in investigations of on-line child exploitation crimes.
  - Yahoo! maintains a 24x7 law enforcement compliance function which responds to requests related to child exploitation in an expedited fashion.
  - We engage in law enforcement educational efforts including presentations for Internet Crimes Against Children investigators, Federal investigators, and state Attorneys General offices.
  - We work with law enforcement and NCMEC to take swift action when we become aware of harmful activities to children that are in violation of our policies.
  - Yahoo! was also an early participant in the Financial Coalition Against Child Pornography, a coalition of credit card issuers and Internet services companies which seeks to eliminate commercial child pornography by taking action on the payment systems used fund these illegal operations.

As evidenced by the many of examples of our engagement on these issues over a number of years, Yahoo! is very much in line with the actions suggested by the OSTWG report. We have found our niche and will continue to work to protect kids online.

#### **Role for Government**

Yahoo! believes government agencies can follow up on the recommendations of the OSTWG report and the findings of our survey by sponsoring additional research, highlighting best practice and safety advice through sites like the FTC's OnGuard Online, encouraging the development of online safety tools, continuing to promote education and training of students and teachers, and maintaining oversight of reporting and enforcement efforts. While many of the other players engaged in this dialogue can educate and create technologies or tools, only the government can enforce the laws passed to fight against child predation and exploitation.

To that end, Yahoo! supports implementation of the provisions of several laws passed in the 110th Congress, including the Protect our Children Act, P.L. 110-401, which provided authorization for new computer forensics labs to assist law enforcement investigations, a new national strategy for child exploitation prevention and interdiction, strengthening the role of ICAC Task Forces, and creation of a Crimes against Children Data System. Additionally, Congress passed the Protecting Children in the 21st Century Act, P.L. 110-385, which authorized an education campaign on child safety to be run by the FTC as well as limitations on funding for schools and libraries unless they have online safety and cyberbullying education. Congress also passed the Kids Act, P.L. 110-400 designed to allow service providers to access lists of sexual predators' screen names, but no rule has yet been established for sharing online identities. Other legislation passed in 2008 and known as the Effective Child Pornography Prosecution Act, P.L. 110-358, included changes to interstate commerce definitions to include child pornography as well as stricter penalties for violations of the law in this area. All of these changes are still in the implementation stage or are awaiting rulemakings and testing in the market and/or courts. It is important for this committee and others in this Congress to ensure the

<sup>12</sup>*Id.* at 88-89.

<sup>13</sup>*Id.* at 116.

laws you have passed are moving forward, as you are doing today by reviewing these issues in depth.

**Conclusion**

Our survey findings are both encouraging and cause for reflection. While parental engagement is overall at a positive level, kids, parents and educators are all struggling with how best to approach the challenging issue of cyberbullying. And parents and kids both need to better understand digital reputation management—the long-term impact of the information they share in the online world.

The OSTWG Report both reinforces the findings from our survey and our ongoing dialogue with safety experts, and suggests additional data and education are needed. Yahoo! is committed to continuing down the path of promoting user awareness and cultivating safe online behaviors among our subscribers. We look forward to continuing the safety dialogue with our partners, peers and law enforcement and, in particular, with this committee. We further look forward to seeing how Congress conducts oversight over the many varied agencies implementing the four new child safety laws enacted in 2008.

Thank you, once again, for taking our testimony on these issues.

**Online Safety and Digital Protection**

**Yahoo! Consumer Pulse Survey—April 2010**

**Background & Methodology**

- Yahoo!, in partnership with Ipsos OTX, conducted an online survey to gain insight into consumers’ behaviors and perceptions with respect to online safety.
- 2003 respondents were recruited via Ipsos OTX’s Internet panel for an 18 minute online survey. Interviews were conducted from April 16–April 21.

Survey sample represented the US online population among persons 18-64.

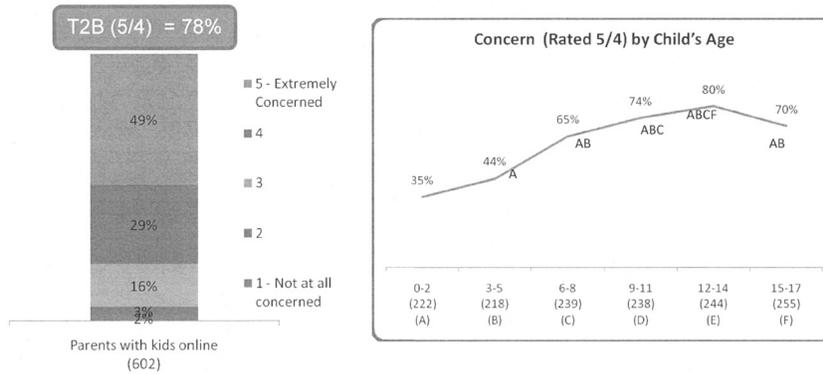


	Total (2003)
Male	50%
Female	50%
Married or Living w Partner	52%
Single, never married	32%
Divorced/Separated/Widowed	14%
Parent of kid 17 or younger	40%
Not Parent of kid 17 or younger	60%
Northeast	20%
Midwest	26%
South	33%
West	19%
Caucasian	69%
African-American	15%
Hispanic or Latino	13%
Asian/Pacific Islander/Other	3%
18-34	39%
35-44	24%
45-54	22%
55-64	15%

**Parents & Kid's Online Safety Management**

**Concern for children's online safety is very high and increases with the age of the child up to 14; Almost 50% of parents with kids online are "very concerned"**

How concerned are you with child's safety online?  
Base: Parents with Kids Online



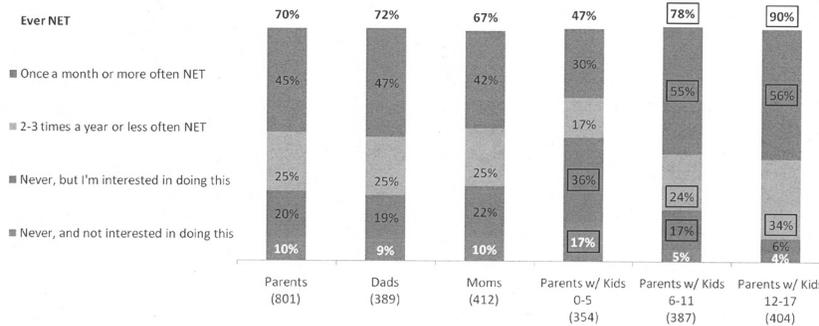
Letters indicate statistically significant differences at the 90 percent confidence level between corresponding groups. PARENT11. On a scale of 1-5 how concerned are you about your child's safety online?

Source: Yahoo! Online Safety & Digital Protection Survey (April 2010)

**Almost half of parents talk to their kids about online safety once a month or more. Dads and those with older kids are more likely to lead the discussion about online safety.**

- Women and those with younger kids are more interested in talking to their kids about online safety.

Frequency of Talking to Kids about Online Safety  
Base: Parents



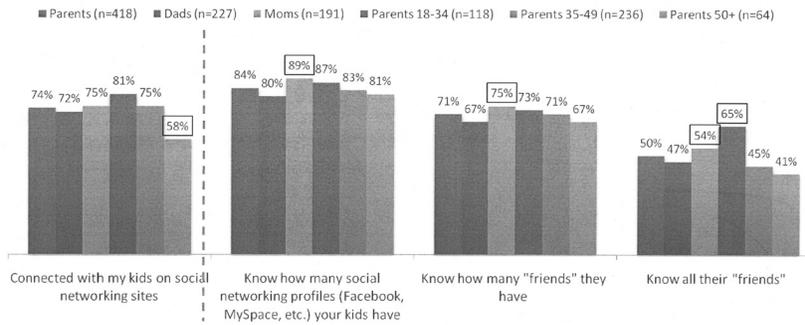
Boxes indicate statistically significant differences at the 90 percent confidence level between corresponding demographic groups. PARENT17. How often do you talk to your child(ren) about online safety?

Source: Yahoo! Online Safety & Digital Protection Survey (April 2010)

### Over 80% of parents who have kids using social networking know the number of profiles their kids have

- About 75% are “friends” with their kids, around 70% know how many “friends” they have and 50% know all of those friends

What do you know about your child’s social network profile?  
Base: Parents with Kids who Visit Social Networking Sites



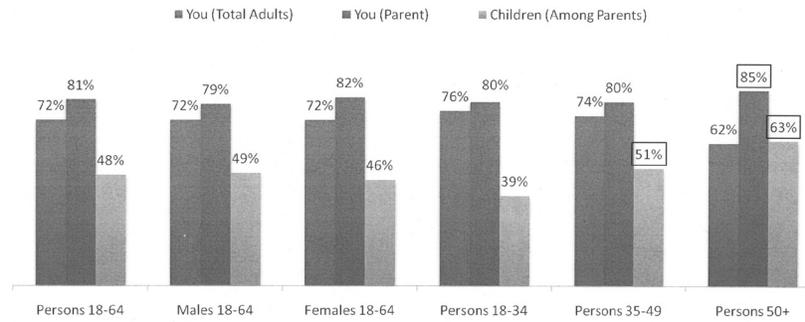
PARENT18. Are you connected ('friends' with) to your kids on social network sites? Base: Children visit social networking sites PARENT19. Which of the following, if any, do you know? Base: Children visit social networking sites.

Source: Yahoo! Online Safety & Digital Protection Survey (April 2010)

### Almost 3 out of 4 adults know what cyber bullying entails. This is especially higher among parents. Of concern, only half of children (according to their parents) are aware of cyber bullying.

Are you aware of cyber bullying?

Base: Total Respondents or Parents



Boxes indicate statistically significant differences at the 90 percent confidence level between corresponding groups.

PARENT5. Do you, and does your child(ren), know what cyber-bullying is? Cyber-bullying, happens when people use the Internet, cell phones, or other devices to send or post text or images intended to hurt or embarrass another person. \*Base: Total Answering—changed mid-field. Source: Yahoo! Online Safety & Digital Protection Survey (April 2010)

**1 in 4 people aware of cyber-bullying have either been victims themselves or know someone else affected. This is especially higher among men and those younger.**

- Dads and younger parents are more likely to have known someone affected by cyber-bullying.

Have you ever witnessed/experienced cyber-bullying?

AMONG TOTAL ASKED	Persons 18-64	Males 18-64	Females 18-64	Persons 18-34	Persons 35-49	Persons 50+
		B	C	D	E	F
<b>Base: Know about Cyber-bullying</b>	1393	699	694	569	505	319
Yes NET	25%	29% <sup>C</sup>	22%	38% <sup>EF</sup>	19% <sup>F</sup>	13%
Yes, I have been a victim	7%	9% <sup>C</sup>	5%	12% <sup>EF</sup>	5% <sup>F</sup>	2%
Yes, my child(ren) has been a victim	2%	2%	2%	1%	2%	3%
Yes, someone I know has been a victim	17%	18%	15%	25% <sup>EF</sup>	12%	9%
No	75%	71%	78% <sup>B</sup>	62%	81% <sup>D</sup>	87% <sup>DE</sup>

AMONG PARENTS ASKED	Total Parents	Total Dads	Total Moms	Parents 18-34	Parents 35-49	Parents 50+
		B	C	D	E	F
<b>Base: Know about Cyber-bullying</b>	646	308	338	251	313	82
Yes NET	28%	33% <sup>C</sup>	22%	40% <sup>EF</sup>	20%	18%
Yes, I have been a victim	8%	12% <sup>C</sup>	4%	14% <sup>EF</sup>	5%	1%
Yes, my child(ren) has been a victim	3%	3%	4%	2%	3%	5%
Yes, someone I know has been a victim	17%	19%	14%	24% <sup>EF</sup>	12%	12%
No	72%	67%	78% <sup>B</sup>	60%	80% <sup>D</sup>	82% <sup>D</sup>

Letters indicate statistically significant differences at the 90 percent confidence level between corresponding groups.

PARENT7. Have you ever witnessed or experienced cyber bullying?

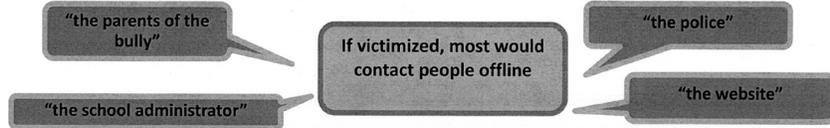
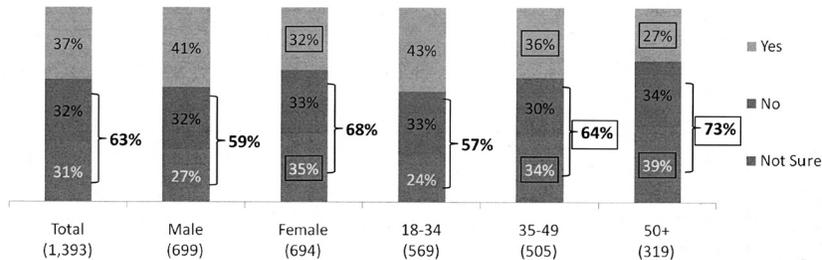
Source: Yahoo! Online Safety & Digital Protection Survey (April 2010)

**Less than 40% of people know what to do about cyber bullying**

- Women and older individuals are even less sure about how to take action

Do you know what to do about cyber bullying?

Base: People aware of cyber bullying



Boxes indicate statistically significant differences at the 90 percent confidence level between corresponding demographic groups.

PARENT8. Do you know what to do about cyber bullying?

OE2: Imagine if you or your child(ren) were the victim of cyber bullying. What, if anything, would you do about it?

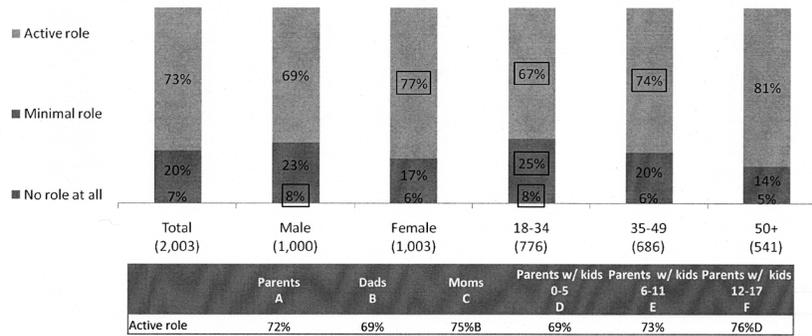
Source: Yahoo! Online Safety & Digital Protection Survey (April 2010)

**Almost three quarters of people want their child’s school to play an active role in teaching kids about online safety and citizenship**

- An even higher percentage of women and older individuals feel the school should take an active approach to this matter.
- This is especially important for parents with kids middle school to high-school aged.

What role should schools play in teaching online safety/citizenship?

Base: Total Respondents



Boxes indicate statistically significant differences at the 90 percent confidence level between corresponding demographic groups.

PARENT24. What role do you think schools should play in teaching children about online safety and citizenship?

Source: Yahoo! Online Safety & Digital Protection Survey (April 2010)

**Most parents do not know if their child’s school has an official policy on this matter . Dads and younger parents are more likely to be in the know.**

Does your children's school have a cyber-bullying policy?

Base: Parents

	Total Parents	Total Dads	Total Moms	Parents 18-34	Parents 35-49	Parents 50+
		B	C	D	E	F
Base	801	389	412	313	392	96
Yes	23%	28%C	19%	26%	21%	23%
No	11%	13%C	9%	12%	11%	8%
Don't know	51%	49%	53%	36%	60%D	62%D
Child(ren) not in school	14%	10%	19%B	26%EF	7%	6%

Lettering indicate statistically significant differences at the 90 percent confidence level between corresponding demographic groups.

PARENT6. Does your child(ren)'s school have a cyber-bullying policy?

Source: Yahoo! Online Safety & Digital Protection Survey (April 2010)

The most common actions parents take to manage children's online behavior involve conversations about respecting the privacy of others and checking on their kids' privacy settings.

- About two thirds of parents, especially fathers and older parents, have taken at least one of these actions to manage their children's online behavior

How have you managed your child's online behavior?

	Total Parents	Total Dads	Total Moms	Parents 18-34	Parents 35-49	Parents 50+
		B	C	D	E	F
<b>Base: Parents</b>	801	389	412	313	392	96
Any NET	67%	71%C	63%	57%	74%D	73%D
Had a conversation with your child about respecting the privacy of their friends (e.g. not posting or tagging photos without their permission)	39%	39%	40%	30%	45%D	49%D
Checked your kids' privacy settings on social networks or websites	38%	38%	38%	31%	45%DF	30%
Have a conversation/talk to your kids about "sexting" (i.e. act of sending/receiving sexually explicit pictures or messages to others via mobile devices)	35%	35%	34%	24%	40%D	49%D
Had a conversation with your child and/or helped them set up privacy settings on social networking sites	33%	34%	32%	26%	37%D	39%D
Had a conversation with your child about cyber bullying	32%	32%	32%	27%	34%D	45%DE
Had a conversation with your child about their digital reputation/footprint	26%	30%C	22%	24%	26%	31%
Check videos your children have posted to YouTube or other sites	26%	28%	24%	18%	30%D	30%D
Talked to your child about how they can build a positive digital footprint (e.g. blogging, writing fan fiction, creating music, volunteering, etc.)	22%	24%	20%	20%	20%	31%DE
None of these	33%	29%	37%B	43%EF	26%	27%

PARENT9. Which of the following have you done?

Source: Yahoo! Online Safety & Digital Protection Survey (April 2010)

The large majority of parents monitor their children's phone and internet use in some way; Many check to see where their kids are searching, set time limits, set parental controls, and use filters.

- Dads are more likely set up filters, monitor text messages/# of text messages and use software.

What do you do regarding your kid's use of the internet/cell phones?

	Total Parents	Total Dads	Total Moms	Parents 18-34	Parents 35-49	Parents 50+
		B	C	D	E	F
<b>PARENTIAL CONTROLS</b>						
<b>Base: Parents</b>	801	389	412	313	392	96
Any NET	91%	91%	91%	92%	91%	89%
Check to see where online your children are searching	49%	48%	49%	39%	56%D	50%D
Set time limits for your children's use of computers or cell phones	43%	42%	44%	38%	50%DF	35%
Set parental controls on video sites	39%	40%	37%	36%	41%	34%
Use some kind of filters to limit where you kids go on the web	35%	39%C	32%	32%	39%D	31%
Have a family media agreement in your home (e.g. one that provides guidelines for when and how long to use the computer, what sites are safe to visit, what types of information to post online)	28%	30%	26%	27%	28%	29%
Monitor the time your child sends text messages	25%	29%C	20%	24%	25%	26%
Monitor how many text messages your child sends	23%	29%C	17%	22%	24%	22%
Require your children to turn in their cell phone/computer at night so that they don't have them in their bedrooms	22%	24%	21%	20%	24%	21%
Use some kind of software to monitor where you kids go on the web	22%	26%C	18%	22%	22%	21%
My child does not own a cell phone/computer	20%	16%	24%B	31%EF	12%	15%
None of these	9%	9%	9%	8%	9%	11%

Lettering indicate statistically significant differences at the 90 percent confidence level between corresponding demographic groups.

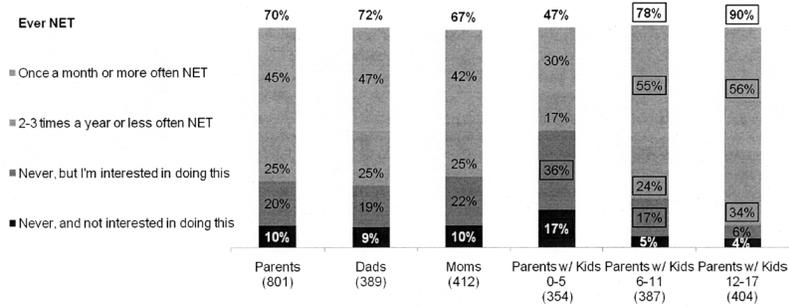
PARENT3. Which of the following, if any, regarding your kid's use of the Internet and cell phones do you do?

Source: Yahoo! Online Safety & Digital Protection Survey (April 2010)

**Almost half of parents talk to their kids about online safety once a month or more. Dads and those with older kids are more likely to lead the discussion about online safety.**

- Women and those with younger kids are more interested in talking to their kids about online safety.

Frequency of Talking to Kids about Online Safety  
Base: Parents



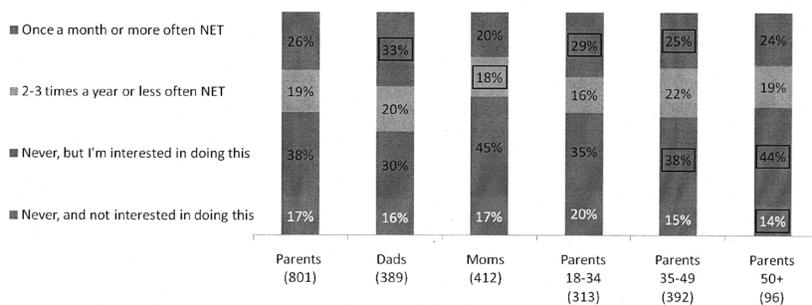
Boxes indicate statistically significant differences at the 90 percent confidence level between corresponding demographic groups.

PARENT17. How often do you talk to your child(ren) about online safety?  
Source: Yahoo! Online Safety & Digital Protection Survey (April 2010)

**More than half of parents have never done a search for their kid's name online, but most of these people are interested in doing so**

- Fathers search for their kids' names more often than mothers, but the women are interested in starting

How frequently do you search your children's name online?  
Base: Parents



PARENT15. How often, if ever, do you search your children's name online to see what comes up or to check his/her profile? Base: Parents Boxes indicate statistically significant differences at the 90 percent confidence level between corresponding demographic groups.

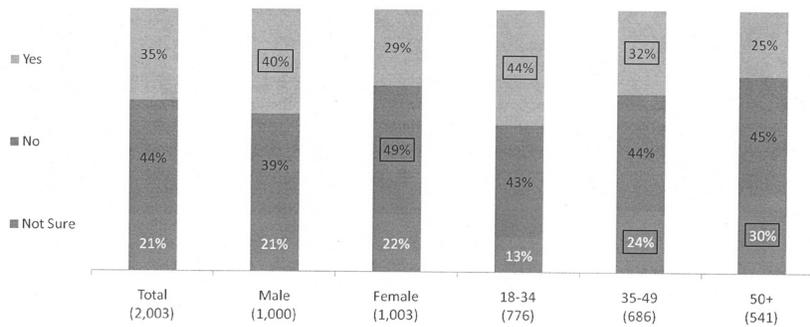
Source: Yahoo! Online Safety & Digital Protection Survey (April 2010)

**Adult Online Image Management**

**Two-thirds of people do not know what a digital footprint is.**

- In line with their pattern of enhanced tech savviness, men and younger individuals are more familiar with this term

Do you know what a “digital footprint” is?  
Base: Total Respondents



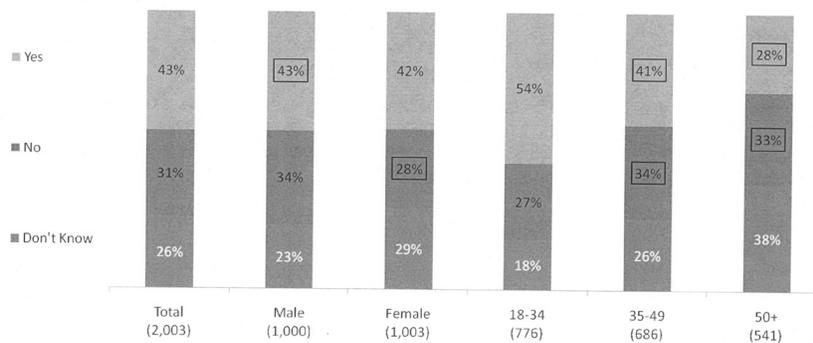
Boxes indicate statistically significant differences at the 90 percent confidence level between corresponding demographic groups.

PROFPR13. Do you know what a digital footprint is?  
Source: Yahoo! Online Safety & Digital Protection Survey (April 2010)

**Fewer than half of consumers feel they are in control of their online image**

- Younger individuals, especially 18-34 year olds, feel more in-control than others

Are you in control of your image online?  
Base: Total Respondents



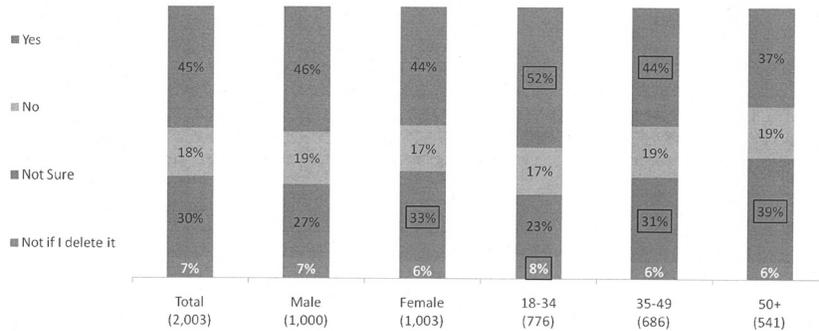
Boxes indicate statistically significant differences at the 90 percent confidence level between corresponding demographic groups.

PROFPR15. Do you think you are in control of your online image (i.e., the image you portray online)?  
Source: Yahoo! Online Safety & Digital Protection Survey (April 2010)

### Less than half of respondents realize that the information they put on the web will remain online forever

- Again, women and older individuals are less sure about this

Will your posts/comments remain online forever?  
Base: Total Respondents



Boxes indicate statistically significant differences at the 90 percent confidence level between corresponding demographic groups.

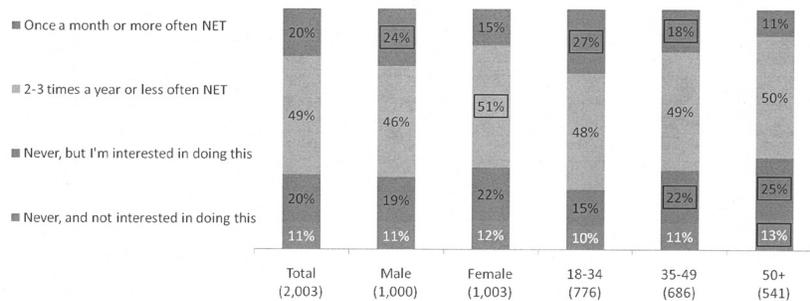
PROFPRO4. When you send an e-mail or post a comment on someone's wall or a blog, do you think it will remain online forever?

Source: Yahoo! Online Safety & Digital Protection Survey (April 2010)

### Most people plug their own name into a search engine no more than two to three times a year

- Men and younger people are more likely to do this once a month or more
- Older individuals are more likely never to have tried this, but they are interested in doing so

How frequently do you search your own name online?  
Base: Total Respondents



Boxes indicate statistically significant differences at the 90 percent confidence level between corresponding demographic groups.

PROFPRO10. How often, if ever, do you search online your own name to see what comes up or to check your profile?

Source: Yahoo! Online Safety & Digital Protection Survey (April 2010)

**Under 50 year olds are most proactive about managing their digital profile**

How do you manage your digital profile?

Base: Total Respondents

	Persons 18-64 A	Male 18-64 B	Female 18-64 C	Persons 18-34 D	Persons 35-49 E	Persons 50+ F
<b>Base: Total Respondents</b>	<b>2003</b>	<b>1000</b>	<b>1003</b>	<b>776</b>	<b>686</b>	<b>541</b>
Limit my personal information available on my social networking site/blog	49%	43%	55%B	52%F	48%	45%
Keep strict privacy settings on my social networking site/blog	38%	35%	42%B	45%EF	39%F	27%
Avoid allowing people access to my blog/social networking site unless I know them personally	35%	30%	39%B	42%EF	33%F	26%
I looked myself up using a search engine to see what information was out there about me	31%	30%	33%	33%	33%F	27%
Limit the type/number of photos/video uploaded by myself	29%	28%	29%	31%F	30%F	23%
Limit/prevent others from posting anything on my blog/social networking site	18%	18%	17%	22%EF	18%F	12%
Remove 'tag' on photos/video of me uploaded by other people	14%	14%	14%	21%F	13%F	6%
Deleted a blog/soc. networking page	13%	16%C	11%	18%EF	12%F	8%
Cancelled another online account	13%	14%	12%	18%EF	12%F	8%
Conducted a thorough check of everywhere on the Internet my name or personal information showed up	12%	14%	11%	14%F	14%F	9%
None of these	22%	23%	21%	16%	24%D	28%DE

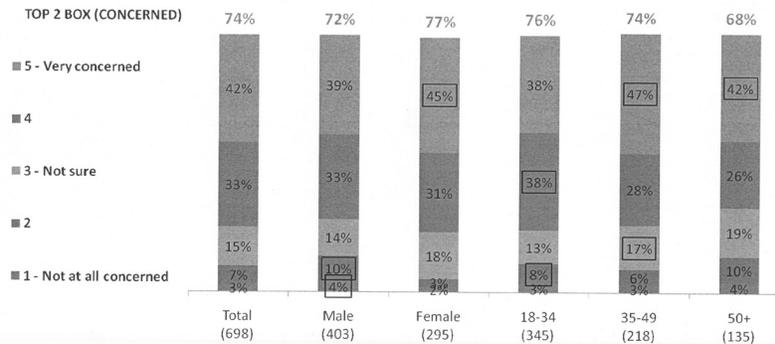
Lettering indicate statistically significant differences at the 90 percent confidence level between corresponding demographic groups.

DIGFTPR5. Which, if any, of the following steps do you take to manage your “digital profile”?  
Source: Yahoo! Online Safety & Digital Protection Survey (April 2010)

**3 out of 4 among those who know what a digital footprint is are concerned with protecting their digital profile**

- Women and older individuals are more concerned than men and younger individuals

How concerned are you in protecting your digital profile from fraud/misuse? Base: Among Those Aware of Digital Footprint



Boxes indicate statistically significant differences at the 90 percent confidence level between corresponding demographic groups.

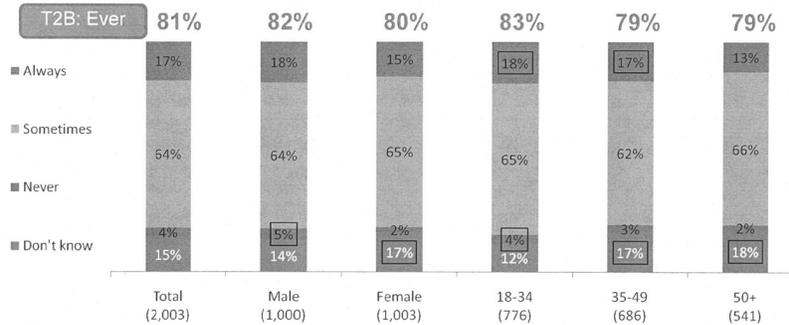
DIGFTPR4. How concerned are you about protecting your “digital profile,” to guard against identity theft or other fraud/misuse/abuse?

Source: Yahoo! Online Safety & Digital Protection Survey (April 2010)

### The large majority of respondents feel that personal information found online is sometimes used to make important decisions (such as hiring)

- Again, women and older individuals responded “Don’t know” more often than men and younger people

How frequently is online info used to make important decisions?  
Base: Total Respondents



Boxes indicate statistically significant differences at the 90 percent confidence level between corresponding demographic groups.

PROFPRO9. How often do you think that information found online about people is used to make a hiring or other important decision?

Source: Yahoo! Online Safety & Digital Protection Survey (April 2010)

### People are more concerned about cyber criminals seeing their personal information online than they are about anyone else

- Young people are the most concerned about all types of people seeing their personal information – a disparity probably driven by their higher use of revealing sites, like social networking.

Whom are you most concerned seeing your personal info online?  
Base: Total Respondents

	Persons 18-64 A	Male 18-64 B	Female 18-64 C	Persons 18-34 D	Persons 35-49 E	Persons 50+ F
Cyber criminals	69%	66%	71%	65%	70%	72%D
Prospective employer	20%	20%	20%	27%EF	16%	15%
Ex-spouse/former girlfriend/boyfriend	19%	17%	20%	22%F	20%F	13%
Current employer	14%	16%	13%	19%EF	13%F	9%
Family members	11%	12%	11%	16%EF	10%F	7%
Significant other	7%	9%C	6%	11%EF	5%	6%
Your children	7%	9%C	6%	8%F	9%F	5%
Not concerned about anyone seeing my personal information online	19%	21%	18%	19%	17%	23%E

Lettering indicate statistically significant differences at the 90 percent confidence level between corresponding demographic groups.

PROFPRO6. Whom are you most concerned will see your personal information online? Select all that apply.

Source: Yahoo! Online Safety & Digital Protection Survey (April 2010)