WORKING GROUP · JUNE 2010 · ONLINE SAFETY AND TECHNOLOGY WORKING GROUP · JUNE 2010 · ONLINE SAFETY AND TECHNOLOGY WORKING GROUP · JUNE 2010 · ONLINE SAFETY AN

Youth Safety ON A LIVING INTERNET:

REPORT OF THE ONLINE SAFETY AND TECHNOLOGY WORKING GROUP

ONLINE SAFETY AND TECHNOLOGY WORKING GROUP · JUNE 2010 · ONLINE SAFETY AND TECHNOLOGY WORKING GROUP · JUNE 2010 · ONLINE SAFETY AND TECHNOLOGY WORKING GROU

YOUTH SAFETY ON A LIVING INTERNET:
REPORT OF THE ONLINE SAFETY AND TECHNOLOGY WORKING GROUP

JUNE 4, 2010

To: **The Honorable Lawrence E. Strickling**
Assistant Secretary of Commerce

The Honorable John D. Rockefeller IV, Chairman
Senate Committee on Commerce, Science and Transportation

The Honorable Kathryn Ann Bailey Hutchison, Ranking Member
Senate Committee on Commerce, Science and Transportation

The Honorable John F. Kerry, Chairman
Senate Commerce Subcommittee on Communications, Technology, and the Internet

The Honorable John Ensign, Ranking Member
Senate Commerce Subcommittee on Communications, Technology and the Internet

The Honorable Henry Waxman, Chairman
House Committee on Energy and Commerce

The Honorable Joe Barton, Ranking Member
House Committee on Energy and Commerce

The Honorable Rick Boucher, Chairman
House Commerce Subcommittee on Communications, Technology and the Internet

The Honorable Cliff Stearns, Ranking Member
House Commerce Subcommittee on Communications, Technology and the Internet

From: **Hemanshu Nigam**, Co-Chair
Online Safety and Technology Working Group

Anne Collier, Co-Chair
Online Safety and Technology Working Group

Date: June 4, 2010

On behalf of the Online Safety and Technology Working Group (OSTWG), we are pleased to transmit this report to you. As mandated, we reviewed and evaluated:

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 report contains recommendations in each of the above categories, as well some general recommendations. We believe these recommendations will further advance our collective goal to provide a safer online experience to our children.

We would like to personally thank the support of the National Telecommunications and Information Administration (NTIA) and its staff during this process. Their assistance throughout the past year was invaluable in allowing us to execute on our mandate. We would also like to recognize the leadership of our subcommittee chairs, Christopher Bubb, Larry Magid, Michael McKeehan, and Adam Thierer – each worked diligently to bring much consensus into the final report. We also want to thank the OSTWG members for the tremendous effort they put into their work all the while doing it in a most collaborative fashion. And finally, we would like to recognize the insight offered by representatives from the White House, the Department of Commerce, the Department of Education, the Department of Justice, the Federal Communications Commission, and the Federal Trade Commission.

As co-chairs we have been honored to have led the OSWTG on this journey, and we all look forward to working with you in bringing these recommendations to life – our nation's youth deserve no less.

////

THE ONLINE SAFETY AND TECHNOLOGY WORKING GROUP

CO-CHAIRS

Anne Collier
Co-Director
ConnectSafely.org
President
Net Family News, Inc.

Hemanshu Nigam
Founder
SSP Blue
Formerly Chief Security Officer
News Corporation

MEMBERS

Parry Aftab, Esq.
Founder and Executive Director
WiredSafety.org

Elizabeth Banker
Vice President and General Counsel
Yahoo! Inc.

Christopher Bubb
Assistant General Counsel, Public Safety and Criminal Investigations
AOL

Braden Cox
Policy Counsel
NetChoice Coalition

Caroline Curtin
Policy Counsel, Federal Affairs
Microsoft

Brian Cute
Vice President, Discovery Services
Afilias

Jeremy S. Geigle
President
Arizona Family Council

Marsali Hancock
President
Internet Keep Safe Coalition

Michael Kaiser
Executive Director
National Cyber Security Alliance

Christopher M. Kelly
Formerly Chief Privacy Officer and Head of Global Policy
Facebook

Brian Knapp
Chief Operating Officer
Loopt

Hedda Litwin
Cyberspace Law Counsel
National Association of Attorneys General

Timothy M. Lordan
Executive Director and Counsel
Internet Education Foundation

Larry Magid
Co-Director
ConnectSafely.org

Brian Markwalter
Vice President of Technology and Standards
Consumer Electronics Association

Michael W. McKeehan
Executive Director, Internet and Technology Policy
Verizon

Samuel C. McQuade III
Associate Professor
Rochester Institute of Technology

Orit H. Michiel
Vice President and Domestic Counsel
Motion Picture Association of America

John Morris
General Counsel
Center for Democracy and Technology

Jonathan Nevett
Vice President of Policy and Ethics
Network Solutions, LLC

Jill L. Nissen
Formerly Vice President and Policy Counsel
Ning, Inc.

Jay Opperman
Senior Director of Security and Privacy
Comcast Corporation

Kevin Rupy
Director of Policy Development
USTelecom

John Shehan
Executive Director, Exploited Child Division
National Center for Missing and Exploited Children

Dane Snowden
Vice President, External and State Affairs
CTIA – The Wireless Association

Adam Thierer
President
Progress and Freedom Foundation

Patricia E. Vance
President
Entertainment Software Rating Board

Ralph James Yarro III
Founder, President, and CEO
Think Atomic, Inc.

FEDERAL GOVERNMENT REPRESENTATIVES

Paul R. Almanza
Deputy Chief
Child Exploitation and Obscenity Section
Criminal Division
Department of Justice

Robert Cannon
Senior Counsel for Internet Law
Office of Strategic Planning and Policy Analysis
Federal Communications Commission

Cheryl Petty Garnette
Director
Technology in Education Programs
Office of Innovation and Improvement
Department of Education

Nat Wood
Assistant Director
Division of Consumer and Business Education
Bureau of Consumer Protection
Federal Trade Commission

TABLE OF CONTENTS

EXECUTIVE SUMMARY

The Internet is a living thing. It mirrors and serves as a platform for a spectrum of humanity's lives, sociality, publications and productions. And as with all living things, its current state is guided and molded by the years of evolution it has gone through to reach its current place in our society. Tasked with the goal of examining the safety of this dynamic medium, the Online Safety and Technology Working Group (OSTWG) embraced its mission mindful of the great amount of work done before it. We approached our task with open eyes and open minds, while at the same time remaining aware of the many efforts that had gone before us, many of which individual OSTWG members had participated in. Still, we were determined to take our combined knowledge and insights gained over the past year to shed new light on the issues reflected in our recommendations to you.

The OSTWG was fortunate to have representatives from nearly every facet of the child online safety ecosystem represented. Members came from the Internet industry, child safety advocacy organizations, educational and civil liberties communities, the government, and law enforcement communities. Collectively, we brought to our work more than 250 years of experience in online safety from a spectrum of varying perspectives. We hope the set of recommendations we are delivering to you here will leave an indelible mark on the online experiences of our country's children as they evolve into adults in this digital century.

The OSTWG was established by the "Broadband Data Improvement Act" (the Act), Pub. L. No. 110–385. Section 214 of the Act, which was signed into law on October 10, 2008, mandated the NTIA to create the OSTWG, bringing this group together to focus on four different components of online safety.

Specifically, the OSTWG was established to review and evaluate:

- 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;
- 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;
- The practices of electronic communications service providers and remote computing service providers related to record retention in connection with crimes against children; and
- The development of technologies to help parents shield their children from inappropriate material on the Internet.

The Act specifies that the OSTWG must be comprised of up to 30 members who are "representatives of relevant sectors of the business community, public interest groups, and other appropriate groups and Federal agencies." This business community includes, at a minimum, Internet service providers, Internet content providers (especially providers of content for children), producers of blocking and filtering software, operators of social networking sites, search engines, Web portals, and domain name service (DNS) providers. Public interest groups may include organizations that work on behalf of children or study children's issues, Internet safety groups, and education and academic entities. The NTIA sought representatives from a broad spectrum of organizations to obtain the best information

available on the state of online safety. The OSTWG would also include representatives from various federal agencies. While federal agency members provided information and contributed to discussions at OSTWG meetings, the recommendations in this report do not necessarily represent the policy positions of the agencies or their leadership.

The full list of members is included in Appendix A. It is clear from the make-up of the OSTWG that the NTIA was successful in executing on this mandate of the Act. For that we are grateful, as it allowed for a multi-dimensional examination of the issues set before us.

OSTWG SUBCOMMITTEES

In order to provide you with a complete picture and set of recommendations in each of the areas outlined by the Act, we created a subcommittee for each topic put forth in the statute, each led by a subcommittee chair. Lawrence J. Magid led the Education subcommittee, Michael W. McKeehan led the Data Retention subcommittee, Christopher G. Bubb led the Child Pornography Reporting subcommittee, and Adam Thierer led the Technology subcommittee. Following an introductory meeting on June 4, 2009, we held meetings where each subcommittee invited experts to provide valuable insight to inform the work of that particular subcommittee. These meetings were held on September 24, 2009, November 3, 2009, February 4, 2010, and May 19, 2010. All meetings were held in Washington, D.C. and were open to the public and news media. The agenda for each of these subcommittee meetings is available in Appendix B as well as online on the Web.[1]

SPECIAL SPEAKERS

To build on the work of preceding task forces, give context to our work, and receive the most current thinking and research on youth Internet use, we invited a special guest to speak at each of our meetings. Here's a short summary of what each speaker said:

At our first meeting on June 4, 2009, Susan Crawford, JD, Assistant to the President for Science, Technology and Innovation and a member of the National Economic Council, called on this Group to focus on research-based education – of both parents and children – as a key to children's online safety. "I love this line, and I am going to repeat it: 'The best software is between the ears'," Crawford said. She asked us to "avoid the overheated rhetoric about risks to kids online," "insensitivity to the constitutional concerns that legitimize use of the Internet," and "one-size-fits-all solutions." She added that government does not have a very good track record with "technological mandates."

On September 24, 2009, Dr. Henry Jenkins, author and media professor at the University of Southern California, also cautioned us against sensationalist media coverage of digital teens. He said that what he and his fellow researchers of the $50 million McArthur Digital Youth Project have seen is that "most young people are trying to make the right choices in a world that most of us don't fully understand yet, a world where they can't get good advice from the adults around them, where they are moving into new activities that were not part of the life of their parents growing up – very capable young people who are doing responsible things, taking advantage of the technologies that are around them." Jenkins said teens are engaged in four activities "central to the life of young people in participatory culture: circulating media, connecting with each other, creating media, and collaborating with each other." It is crucial, he said, to bring these activities into classrooms nationwide so that all young people have equal opportunity to participate. This is crucial, too, because young people "are looking for

1 NTIA Web site (http://www.ntia.doc.gov/advisory/onlinesafety/)

guidance often [in their use of new media] but don't know where to turn," Jenkins told us. In focusing so much on blocking new media from school as a protection, schools are failing to do with today's media what they have long done for students with traditional media – enrich and guide their use. Finally, Jenkins asked us to take up "the ethics challenge" – creating the conditions for youth to absorb and learn in social-media projects and environments the kind of personal and professional ethics young people used to learn while working on high school newspapers.

"Digital ethics" was the focus of sociologist Carrie James's presentation at our November 3, 2009, meeting. Dr. James, research director at the Harvard University School of Education's GoodPlay Project, said, "There are also a lot of confused kids out there, some of them mal-intentioned perpetrators, but arguably more making naïve - and ethically ambiguous - choices that can hold serious ethical consequences." Seeming to reinforce Jenkins's observation at the previous meeting, she told us there is a dearth of ethical supports for youth in social media. More than 60% of GoodPlay's research sample named a parent, teacher or coach as a mentor or strong influence in their offline lives, but few adults were mentioned as guides in their social media use. Her research group found it "promising" that "nearly a third of the sample named a peer mentor" for their online experiences, but that's not promising, she said, "if ethical thinking is rare among peers online." With USC's New Media Literacies Project, the GoodPlay Project has released a casebook, *Our Space: Being a Responsible Citizen of the Digital World*, for educators focusing on two facets of ethics online, the latter having a great deal to do with online safety on the social Web: "Whether and how youth behave ethically themselves, and how they can protect themselves against unethical, irresponsible behavior of others."

The day before our February 4, 2010, meeting, Amanda Lenhart, senior research specialist at the Pew Internet & American Life Project, had released research on young people's use of the social Web, both fixed and mobile, finding that 93% of American teens (12-to-17-year-olds) use the Internet, 73% use social network sites, and 75% of them own cell phones. As for the newest tech-related risk to youth, so-called "sexting," Lenhart said at our meeting that her research had found that 4% of American teens have sent sexually suggestive images or videos of themselves via cell phone, and 15% have received such images from someone they know, with no gender differences in those percentages.

BACKGROUND & CONTEXT

The Internet, what we know about youth online risk, and the task of keeping online youth safe have all changed significantly in the 10 years since the COPA Commission reported to Congress.

From the perspective of today's increasingly user-driven multi-dimensional media environment, the task the COPA Commission was charged with what might today be considered a supremely simple one: to study "various technological tools and methods for protecting minors from material that is harmful to minors." At the time, however, during that "Web 1.0" era, when users were largely consumers rather than the producers, socializers, and communicators they have now become, examining potential solutions to even a single online risk, inappropriate content, seemed a big task.

So did that of the National Research Council, whose Computer Science and Telecommunications Board in 2002 conducted the study "Youth, Pornography, and the Internet."[2] Edited by former U.S. Attorney General Dick Thornburgh and Herbert S. Lin, the "Thornburgh Report" examined the issue of children's exposure to sexually explicit material online from multiple perspectives and reviewed a number of approaches to protecting children from encountering such material. The report concluded

2 "Youth, Pornography, and the Internet," Dick Thornburgh and Herbert S. Lin, editors, Computer Science and Telecommunications Board, National Research Council, 2002 (http://www.nap.edu/readingroom.php?book=youth_internet&page=index.html)

that "developing in children and youth an ethic of responsible choice and skills for appropriate behavior is foundational for all efforts to protect them – with respect to inappropriate sexually explicit material on the Internet as well as many other dangers on the Internet and in the physical world. Social and educational strategies are central to such development, but technology and public policy are important as well – and the three can act together to reinforce each other's value." The report encapsulated this finding into the oft-quoted and succinct "swimming pool analogy," acknowledging the protective value of fences around pools while asserting that such "technology" could never replace the life-long protection of teaching kids how to swim.

Fast-forward six years to the next national youth-online-safety task force, that of Harvard University Law School's Berkman Center for Internet & Society, assembled in 2008 and officially called the Internet Safety Technical Task Force (ISTTF). In the highly charged Net-safety climate of that time, fears of predators in a "new phenomenon" called social networking sites were running high among parents and policymakers alike. The ISTTF, too, was charged with a more specific task than ours: examine the state of online identity-authentication technology and other online safety tools that would inform online safety for minors on the social Web. The charge, however, implied a prescribed solution that had not had the benefit of a thorough diagnosis. Consequently, in addition to a review of current age-verification products and technologies, the Internet Safety & Technical Task Force, wisely undertook a comprehensive review of academic research on youth risk online up to 2008.

The ISTTF's top two findings[3] – that "sexual predation on minors by adults, both online and offline, remains a concern" but that "bullying and harassment, most often by peers, are the most frequent threats that minors face, both online and offline" – point not just to the OSTWG's challenge but that of anyone charged with analyzing online safety solutions today – the need for better questions, based on a greater understanding of the nature of the Internet today and how youth use it.

What these two findings on the part of the ISTTF suggest is not only that, thanks to the growing body of youth-online-risk research, we are now able to seek solutions as a society which are fact-based, not fear-based, but also that minors themselves – mainly pre-teens and teens (though the tech-literacy age is going down) – have a role to play in improving their own safety online and that of their peers.

For example, the ISTTF found that "many of the threats that youth experience online are perpetrated by their peers, including sexual solicitation and online harassment." The report also cited more than a dozen times a 2007 study published in Archives of Pediatrics & Adolescent Medicine[4], which found that "youth who engage in online aggressive behavior ... are more than twice as likely to report online victimization."

It is clear, then, that the definition of "youth online safety" has broadened and become more complex in the past 10 years, as have the role of the online user and the inter-connected devices today's user takes advantage of when consuming, socializing, producing, and connecting. In addition to cyberbullying, inappropriate content, and predation, other risks have emerged, including "sexting" and the risks related to geolocation technology in online applications and on mobile phones. Thus, we are forced to either create a new taxonomy of online safety, or at the very least, expand our historical definition. While many possibilities exist – simply to make the point more obvious – here is one

3 "Enhancing Child Safety & Online Technologies: Final Report of the Internet Safety Technical Task Force to the Multi-State Working Group on Social Networking of State Attorneys General of the United States," the Berkman Center for Internet & Society at Harvard University, December 31, 2008 (http://cyber.law.harvard.edu/sites/cyber.law.harvard.edu/files/ISTTF_Final_Report-Executive_Summary.pdf)

4 "Internet Prevention Messages: Targeting the Right Online Behaviors," by Michele L. Ybarra, Kimberly J. Mitchell, David Finkelhor, and Janis Wolak, Archives of Pediatrics & Adolescent Medicine, February 2007 (http://archpedi.ama-assn.org/cgi/content/full/161/2/138)

example of a taxonomy focused less on specific technologies or devices and more on the categories of safety desired:

- **Physical safety** – freedom from physical harm
- **Psychological safety** – freedom from cruelty, harassment, and exposure to potentially disturbing material[5]
- **Reputational and legal safety** – freedom from unwanted social, academic, professional, and legal consequences that could affect users for a lifetime
- **Identity, property, and community safety** – freedom from theft of identity & property

This in no way diminishes the importance of any single form of safety, but it does demonstrate the complexity of our task as a society to ensure young people's safety on the fixed and mobile Internet. And, because of the key role young people increasingly play in their own safety online, it also points to the growing importance of online citizenship and media-literacy education, in addition to what has come to be seen as online safety education, as solutions to youth risk online.

Other important factors that need to be considered by any task force or working group present and future:

- There's no one-size-fits-all, once-and-for-all solution to providing children with every aspect of online child safety. Rather, it takes a comprehensive "toolbox" from which parents, educators, and other safety providers can choose tools appropriate to children's developmental stages and life circumstances, as they grow. That toolbox needs to include safety education, "parental control" technologies such as filtering and monitoring, safety features on connected devices and in online services, media ratings, family and school policy, and government policy. In essence, any solution to online safety must be holistic in nature and multi-dimensional in breadth.
- To youth, social media and technologies are not something extra added on to their lives; they're embedded in their lives. Their offline and online lives have converged into one life. They are socializing in various environments, using various digital and real-life "tools," from face-to-face gatherings to cell phones to social network sites, to name just a few.
- Because the Internet is increasingly user-driven, with its "content" changing in real-time, users are increasingly stakeholders in their own well-being online. Their own behavior online can lead to a full range of experiences, from positive ones to victimization, pointing to the increasingly important role of safety education for children as well as their caregivers. The focus of future task forces therefore needs to be as much on protective education as on protective technology.
- The Internet is, in effect, a "living thing," its content a constantly changing reflection not only of a constantly changing humanity but also its individual and collective publications, productions, thoughts, behaviors, and sociality.

Based on this "snapshot" of the Internet as we are experiencing it right now, the best solutions for promoting child safety, security, and privacy online must be the result of an ongoing negotiation involving all stakeholders: providers of services and devices, parents, schools, government, advocates, healthcare professionals, law enforcement, legislators, and children themselves. All have a role and responsibility in maximizing child safety online.

5 We chose the term "disturbing" to signify a broad and encompassing meaning that includes what could be disturbing when viewed by a minor and what parents may consider to be disturbing for their own children. We did not use the term "harmful," given its more narrowly defined meaning that has resulted from legal court opinions and its use in federal statutes.

SUMMARIES OF THE SUBCOMMITEE REPORTS

In order to fully grasp the breadth and depth of the findings and recommendations of the four subcommittees, it is important to read the full report of each subcommittee in the body of this document. The following only briefly summarizes their findings and recommendations.

SUBCOMMITTEE ON INTERNET SAFETY EDUCATION

Summary

In the late '90s, experts advised parents to keep the family Internet connected computer in a high-traffic part of the house, but now parents must account for Internet access points built into many digital devices, including cell phones. Research has told us that many of the early significant concerns regarding children and their use of the Internet, such as predation, exist but not nearly in the prevalence once believed. Other risks, such as cyberbullying, are actually much more common than thought – starting as early as 2nd grade for some children. Meanwhile, "new" issues such as "sexting" garner a great deal of media attention, though recent studies suggest it is not quite as common as initially believed. Given all the above and the finding of the preceding task force (the ISTTF) that not all youth are equally at risk, it now seems clear that "one size fits all" is not a good strategy. Instead, a strong argument can be made for applying the Primary/Secondary/Tertiary model used in clinical settings and risk-prevention programs to Internet safety. This "levels of prevention" method would represent a tailored and scalable approach and factor in the high correlation between offline and online risk. The approach would also work in concert with non-fear-based, social-norms education, which promotes and establishes a baseline norm of good behavior online.

Research also shows that civil, respectful behavior online is less conducive to risk, and digital media literacy concerning behavior as well as consumption enables children to assess and avoid risk, which is why this subcommittee urges the government to promote nationwide education in digital citizenship and media literacy as the cornerstone of Internet safety.

Industry, NGOs, schools, and government all have established educational strategies; however effectiveness has not been adequately measured. At the federal level, while significant progress has been made with projects such as OnGuardOnline and NetCetera, more inter-agency coordination, public awareness-raising, and public-/private-sector cooperation are needed for national uptake in schools and local communities.

Recommendations

- Keep up with the youth-risk and social-media research, and create a web-based clearinghouse that makes this research accessible to all involved with online safety education at local, state, and federal levels.
- Coordinate Federal Government educational efforts.
- Provide targeted online-safety messaging and treatment.
- Avoid scare tactics and promote the social-norms approach to risk prevention.
- Promote digital citizenship in pre-K-12 education as a national priority.
- Promote instruction in digital media literacy and computer security in pre-K-12 education nationwide.

- Create a Digital Literacy Corps for schools and communities nationwide.
- Make evaluation a component of all federal and federally funded online safety education programs (evaluation involving risk-prevention expertise).
- Establish industry best practices.
- Encourage full, safe use of digital media in schools' regular instruction and professional development in their use as a high priority for educators nationwide.
- Respect young people's expertise and get them involved in risk-prevention education.

SUBCOMMITTEE ON PARENTAL CONTROLS & CHILD PROTECTION TECHNOLOGY

Summary

There is no quick fix or "silver bullet" solution to child safety concerns, especially given the rapid pace of change in the digital world. A diverse array of protective tools are currently available today to families, caretakers, and schools to help encourage better online content and communications. They are most effective as part of a "layered" approach to child online safety. The best of these technologies work in tandem with educational strategies, parental involvement, and other approaches to guide and mentor children, supplementing but not supplanting the educational and mentoring roles. These products and services need to be designed with the needs of families in mind, being easy to use, accessible, flexible, and comprehensible for the typical parent. Industry should assist by continuing to formulate and refine best practices and self-regulatory systems to empower users with more information and tools so that they can make appropriate decisions for themselves and their families, including product settings that are defaulted in a thoughtful way. Government should avoid rigid, top-down technological mandates and instead enhance funding and encourage collaborative, multi-faceted, and multi-stakeholder initiatives and approaches to enhance online safety via innovation and cooperation.

Recommendations

- Engage in ongoing awareness-building efforts.
- Promote greater transparency for parents as to what sort of content and information will be accessible and recorded with a given product when their children are online.
- Bake parental empowerment technologies and options possible into product development whenever possible.
- Develop a common set of terms, agreed upon by the industry, across similar technologies.
- Promote community reporting and policing on sites that host user-generated content.

SUBCOMMITTEE ON CHILD PORNOGRAPHY REPORTING

Summary

Though mandated to study 42 U.S.C. § 13032, that section was repealed almost immediately after the mandate, and, accordingly, this subcommittee endeavored to compare and contrast § 13032 with its de facto replacement, now codified in 18 U.S.C. §§ 2258A through 2258D via the PROTECT Our

Children Act of 2008. Although § 13032 was a significant step forward in requiring service providers to report apparent child pornography when discovered, it lacked specificity in several key areas, including what additional information relating to the reported content would be valuable for law enforcement and whether any explicit criminal immunity would be granted to service providers who were implicitly tasked with transmitting potentially illegal images to the National Center for Missing and Exploited Children (NCMEC). As service providers as well as NCMEC, law enforcement, and prosecutors gained experienced under § 13032, its shortcomings became even more apparent. Service providers were concerned with the legal implications of transmitting illegal material and, without statutory guidance, law enforcement was often not receiving enough useful information from providers to push investigations forward. Sections 2258A *et seq.* improved on the previous provision by explicitly detailing the types of information service providers could include in a report, granting NCMEC more operational flexibility to route reports received, increasing fines, limiting liability for service providers both criminally and civilly, and quite creatively requiring providers to treat NCMEC's notification of receipt of a report as a request to preserve relevant subscriber information. The Act appears to have had a near instant impact on the volume of reports received by NCMEC, which recorded an increase of 84% from 2008-2009 and, at the time of this report, were on pace for an increase of 78% from 2009-2010.

Recommendations

- Task the appropriate executive agency with the objective to conduct a survey using an empirically reliable method to assess industry efforts to promote online safety by means of the new reporting provisions of § 2258A.
- Encourage outreach by NCMEC, government agencies, advocacy groups, and service providers to promote increased awareness of the PROTECT Our Children Act through education, information sharing efforts, and the establishment of sound practices for reporting and data preservation.
- Encourage nascent or smaller service providers who may lack the necessary networking contacts or experience to seek out meetings with NCMEC and law enforcement concerning the reporting and preservation provisions of the Act.
- Continue to encourage collaboration and information sharing among providers to develop new technologies that disrupt the transfer of online child pornography and facilitate reporting to NCMEC.
- Consider tax credits or other financial incentives to assist service providers in bearing the development and implementation costs associated with securely retaining data outside the course of normal business.
- Consider incentives for service providers to establish wellness programs for the employees who face the task of reviewing disturbing images of child sexual abuse in order to maintain compliance with the mandatory reporting requirements.

SUBCOMMITTEE ON DATA RETENTION

Summary

Data retention is a very contentious subject from a policy angle, fraught with conflicting needs and concerns from the perspective of the three groups represented in this report: law enforcement, industry, and consumer privacy. While law enforcement understands the need to carefully consider

all sides of the issue, they postulate that mandatory data retention sufficient to facilitate the effective investigation of online crimes is ultimately workable and will allow law enforcement to solve more crimes involving the sexual exploitation of children. From the industry perspective, while the cost of data storage has drastically fallen over the years, the true cost of retaining data comes in the form of having to protect ever increasing amounts of end users' private data from smarter and smarter criminals lurking on the Internet. Further assessment of the data preservation features enacted in the PROTECT Our Children Act, industry suggests, should occur before considering mandatory data retention. The consumer privacy perspective offers that in addition to issues regarding free speech, mandatory data retention would be overly broad in that it would cover legitimate users and bad actors alike, would be accessible by subpoena without judicial oversight in many situations, and would create a highly valuable database target for information thieves. In the end, it is about striking a balance between law enforcement's legitimate need to investigate and prosecute crimes against children facilitated by the Internet, end-users' legitimate privacy expectations, and the burden of data storage costs to ISPs and OSPs and their subsequent ability to operate as a business.

Recommendations

- ISPs and OSPs should have regular meetings and engage ICAC task forces and federal law enforcement agencies to cross-train on emerging threats, resolve operational glitches, and develop a set of evolving practices and procedures.
- Privacy concerns regarding vast amounts of stored data must be addressed.
- If they are to occur, data retention debates should happen at the federal level, so as not to add further confusion concerning competing regulations among states.
- Congress should assess the results of the data preservation procedures enacted in the PROTECT Our Children Act before considering mandatory data retention.
- We encourage you to read the full subcommittee reports contained in this document to grasp fully not only the insight contained in them, but also the twenty-six (26) recommendations we have provided.

RECOMMENDATIONS FROM THE CO-CHAIRS

Each of the Online Safety & Technology Working Group's four subcommittees have provided recommendations specific to the statute's requirements. As co-chairs, we had not only the honor of guiding a congressionally mandated working group, but also the challenges that come with such a task. We feel it is important for us to provide some of our learned insight to future task forces that will no doubt follow the OSTWG. With this in mind, we urge Congress to consider a few general recommendations concerning the overall mission of child online safety going forward:

1. **Provide proper support to task forces.** When creating future task forces, we recommend that legislation fully empower the appointed group to accomplish the task with which it's charged. Any congressionally mandated cross-sector child safety panel needs to be backed by the resources needed to succeed – sufficient time, if constrained as we were by the Paperwork Reduction Act, and sufficient resources, such as funds for travel by members and speakers and funds for meeting accommodations and staff support. An unfunded mandate creates obstacles that can easily distract from the great work that such mandates can lead to by placing undue burdens on the citizens called upon to serve the American public.

2. **Fill the prescription**. We have completed the work the statute required, but we suggest that there be follow-through. A report is half the job. Now fill the prescription, taking up or studying the value of all the recommendations in this report and determining a course of action. In order to do this, you might consider another congressional mandate that creates the group or groups to take up this important task.
3. **Create a coordinating body**. Although part of a single administration, government agencies can have different (and sometimes conflicting) views and philosophies concerning approaches to addressing many topics. Especially in the area of online child protection, industry can find itself challenged by these differing or even contending government agencies. We recommend the formation of a sufficiently funded, cross-functional group – representing key government agencies, industry, and NGOs – to help build consensus and coordinate efforts across the sectors.
4. **Review, identify, then publicize federal programs.** Conduct a full review of all child online safety projects and programs the federal government has undertaken. Evaluate these for success and then widely promote outstanding projects, such as Net Cetera and Admongo.gov, as opportunities for public/private sector partnerships in online risk prevention. Then promote the creation of these partnerships.
5. **Take a multi-stakeholder approach.** On any topic concerning today's complex new media environment – from education to law enforcement to parenting to risk prevention – no single stakeholder can represent all the expertise needed. As we said at the beginning, the Internet is a living thing reflecting all of life and, where children are concerned, that includes a spectrum of issues – from learning, child development, sociality, and entertainment at one end to crime and victimization at the other. Please recognize this reality and draw upon diverse expertise in all policymaking.

CONCLUSION

Any report about both the Internet and children is necessarily a freeze frame of a rapidly moving landscape – not only because both the technology and how children use it change so quickly but also because of the rapidly growing bodies of youth-risk and social-media research. Thus, any recommendations about children's online safety must take into account the dynamic nature of this landscape. The OSTWG has attempted to offer recommendations that will stand the test of time by stressing that lawmakers, government, and risk-prevention practitioners rely heavily on the research, as it unfolds, to get an accurate picture of what needs to be addressed when it is being addressed. This is in no way dissimilar to the approach policymakers have taken with our nation's longest living laws and policies, which continue to stand up to historical, behavioral, and technological change.

In closing, we stress once again that in order to fully comprehend the significance of the recommendations OSTWG makes, it is critical to read the entire report. We hope that as law and policy makers do so and continue to factor in an even broader spectrum of expertise than the OSTWG already represents, we will begin as a society the process of figuring out and filling the right prescription for child safety online.

SUBCOMMITTEE ON INTERNET SAFETY EDUCATION

To understand how industry, schools, non-profits and government can best provide Internet safety education, we must first grapple with what it is we're educating about and then tackle how to go about the business of educating. And to do that we need to understand the risks and the way youth actually use the Internet and the social media they access through computers, mobile phones, game consoles and other devices.

A lot has changed since the last major congressionally mandated look at Internet safety. When the Commission on Online Child Protection (COPA) issued its Report to Congress in 2000, there were no social networking sites, cell phones were pretty much limited to making phone calls and the primary perceived risks associated with the Internet were access to pornography and other inappropriate material and the fear of adult predators using the Net to entrap our children. In 2000, "place the computer in a central area of the house" was good advice. But that was before Netbooks, tablets, web-enabled smart phones, Wi-Fi and wide-area wireless networks.

There have also been profound changes in the way young people use technology.
In the ensuing decade, young people's use of the Net has shifted away from being mostly consumers of information to becoming active participants. Social networking and video sites have empowered young people not only to shape their own lives but have a direct impact on the media landscape that affects themselves, their peers and adults as well. In February, 2010, the Pew Internet & American Life Project reported[6] that "73% of wired American teens now use social networking websites," up from 55% two years earlier.

Young people have also gravitated toward mobile devices enabling them to do far more than talk. A 2010 Nielsen study[7] on teen use of text messaging found that American teens send and receive an average of 3,146 text messages a month.

PREDATOR DANGER

Knowing that young people spend a considerable amount of time "hanging out" online, many caring adults – including elected officials – naturally worry that they are at risk from predators that might in some way harm them. And, indeed, there are examples of sting operations by law enforcement (and famously even TV crews) that have been successful in exposing adult "predators" who have made online sexual advances to undercover officers and other adults posing as children and teens. To the extent that young people have received an unwanted sexual solicitations online, data from a 2000 DOJ-funded study and a 2006 follow-up from the Crimes Against Children Research Center (CACRC) at the University of New Hampshire concluded that "youth identify most sexual solicitors as being other adolescents."

That is not to say that unwanted solicitations, whether from an adult or a minor, can't have serious consequences, but studies – including some funded by the U.S. Department of Justice – have shown

6 Pew Internet & American Life Project: Social Media and Young Adults (http://www.pewinternet.org/Reports/2010/Social-Media-and-Young-Adults.aspx?r=1)

7 Nielsenwire: Under-aged Texting: Usage and Actual Cost (http://blog.nielsen.com/nielsenwire/online_mobile/under-aged-texting-usage-and-actual-cost/)

that the statistical probability of a young person being physically assaulted by an adult who they first met online is extremely low.

In a report published in the February/March 2008 issue of *American Psychologist*[8], researchers from CACRC found that "adolescents' use of popular social networking sites such as MySpace and Facebook do not appear to increase their risk of being victimized by online predators. Rather, it is risky online interactions such as talking online about sex to unknown people that increases vulnerability, according to the researchers."

After reviewing peer-reviewed studies, the Berkman Center's Internet Safety Technical Task Force[9] (the "Task Force") last year found that "cases [of adult to child sexual encounters on social networks] typically involved post-pubescent youth who were aware that they were meeting an adult male for the purpose of engaging in sexual activity." The Task Force also concluded that "the risk profile for the use of different genres of social media depends on the type of risk, common uses by minors, and the psychosocial makeup of minors who use them." In its review of the youth-risk literature, the Task Force's Research Advisory Board, made up of distinguished scholars and experts in the field of youth safety, concluded, "Youth identify most sexual solicitors as being other adolescents (48%; 43%) or young adults between the ages of 18 and 21 (20%; 30%) and that youth typically ignore or deflect solicitations without experiencing distress."

CYBERBULLYING

What the Task Force and many researchers did find was that "bullying and harassment, most often by peers, are the most frequent threats that minors face, both online and offline."

"Cyberbullying, as it is called when youth are bullied via computers or mobile phones, is real and is affecting a statistically significant number of American youth. And it can start "as early as the 2nd grade for some children," according to a study conducted by Rochester Institute of Technology.[10] The actual percentage is difficult to pin down, but a 2008 Centers for Disease Control (CDC) *Electronic Media and Youth Violence* issue brief[11] reported that "9% to 35% of young people say they have been the victim of electronic aggression."

Among certain populations the problem is even worse. A study conducted at Iowa State University by Warren Blumenfeld and Robyn Cooper[12] found that 54% of lesbian, gay, bisexual and transgender (LGBT) youth had been victims of cyberbullying within the past 30 days. Forty-five percent of the respondents "reported feeling depressed as a result of being cyberbullied," according to the study's authors. Thirty-eight percent felt embarrassed, and 28% felt anxious about attending school. The authors reported that "more than a quarter (26%) had suicidal thoughts."

NOT ALL AGGRESSIVE BEHAVIOR RISES TO THE LEVEL OF BULLYING

The Centers for Disease Control defined electronic aggression as "any type of harassment or bullying (teasing, telling lies, making fun of someone, making rude or mean comments, spreading rumors,

8 University of New Hampshire Crimes Against Children Research Center: Internet Predator Stereotypes Debunked in New Study (http://www.unh.edu/news/cj_nr/2008/feb/lw18internet.cfm)

9 Internet Safety Technical Task Force: Enhancing Child Safety and Online Technologies (http://cyber.law.harvard.edu/pubrelease/isttf/)

10 Rochester Institute of Technology: A Survey of Internet and At-risk Behaviors (http://www.rrcsei.org/RIT%20Cyber%20Survey%20Final%20Report.pdf)

11 Electronic Media and Youth: A CDC Issue Brief (http://www.cdc.gov/violenceprevention/pdf/EA-brief-a.pdf)

12 Iowa State researchers publish national study on cyberbullying of LGBT and allied youths (http://www.news.iastate.edu/news/2010/mar/cyberbullying)

or making threatening or aggressive comments) that occurs through email, a chat room, instant messaging, a website (including blogs), or text messaging." This is a broader spectrum of behavior than researchers' definition of cyberbullying, which generally refers to unwanted aggression that is repeated over time with an imbalance of power between the perpetrator(s) and the victim (see also the *Journal of Adolescent Health, August 2007*. [13]Others define it as repeated unwanted harassment, or a one-time serious threat of bodily harm such as "I will kill you!", which mirrors many state harassment law approaches.

Cyberbullying is basically the same as real-world bullying, though it has elements that don't exist in the physical world such as anonymity, the ability to impersonate the victim, follow the victim home, embarrass the victim in front of an unseen (and potentially vast) online audience and persist online over a long period of time. Also, cyberbullying is typically psychological rather than physical and it's possible for the bully to remain anonymous. But there is often a link between cyberbullying and real-world bullying. In a 2008 cyberbullying study[14] of middle school students conducted by Sameer Hinduja and Justin Patchin, 82% said that the person who bullied them via technology was either from their school (26.5%), a friend (21.1%), an ex-friend (20%) or an ex-boyfriend or ex-girlfriend (14.1%).

A 2009 study[15] carried out by Harris Interactive on behalf of Cox Communications in partnership with the National Center for Missing & Exploited Children and John Walsh found that approximately 19% of teens say they've been cyberbullied online or via text message and that 10% say they've cyberbullied someone else. The Cox study defined cyberbullying as "harassment, embarrassment, or threats online or by text message," which is actually more consistent with the CDC's definition of "electronic aggression" than with the classical definition of bullying.

While the study didn't address the issue of cyberbullying, there is evidence that overall physical bullying is on the decline. Writing in the *Archives of Pediatrics and Adolescent Medicine*[16], David Finkelhor, Heather Turner, Richard Ormrod, and Sherry Hamby found that 15% of youth (ages 2-17) reported that they were physically bullied in 2008. The good news is that that percentage went down from 22% in 2003. The study also found that the percentage reporting a sexual assault decreased from 3.3% to 2%. Lead author Finkelhor noted that declines in bullying and sexual assault and that these problems have been aggressively targeted by school programs and other prevention efforts in recent years. "This suggests that some of the decline may be the fruits of those programs," he said.

"SEXTING"

There is a lot of concern about young people using cell phones and computers to distribute naked or sexually suggestive pictures of themselves, a practice that recently came to be known as "sexting." Estimates of the extent of the problem have varied widely, but a recent study by the Pew Internet & American Life Project[17] "found that 4% of cell-owning teens ages 12-17 say they have sent sexually suggestive nude or nearly nude images or videos of themselves to someone else via text messaging." Fifteen percent of young respondents "say they have received such images of someone they know via text message."

13 Does Online Harassment Constitute Bullying? An Exploration Of Online Harassment by Known Peers and Online-Only Contacts (http://unh.edu/ccrc/pdf/CV172.pdf)

14 Cyber Bullying Research Center (http://www.cyberbullying.us/research.php)

15 Survey: Teens 'sext' and post personal info. News.com (http://news.cnet.com/8301-19518_3-10272311-238.html)

16 *Archives of Pediatric and Adolescent Medicine:* "Trends in Childhood Violence and Abuse Exposure" (http://www.unh.edu/ccrc/pdf/CV196.pdf)

17 Pew Internet & American Life Project: "Teens and Sexting" (http://www.pewinternet.org/Press-Releases/2009/Teens-and-Sexting.aspx)

While 4% who admit having sent a "sext" is still a large number, it's far from the 20% figure reported in a less rigorous 2009 study that prompted a major news website to write in a headline, "Sexting Shockingly Common Among Teens.[18]"

As we look at the sexting data, it's important to try to view the issue from the perspective of teens. There are certainly teens who have been strongly affected by sexting. *Sexting in America*, a documentary[19] created for MTV's A Thin Line Campaign in February, 2010 depicted sexting's impact on two teens. One teen named Ally was extremely distraught after a picture she sent to an ex-boyfriend was distributed all over school. Another teen, Philip Albert, is suffering the legal consequences of having sent out naked pictures of his 16-year-old girlfriend in a fit of anger in the middle of the night. She took and sent him the photos when he was 17, but he distributed them a month after his 18th birthday, which resulted in criminal charges. He's now on probation and, unless his lawyer is successful in getting the court to take him off the list, he could remain on the registered sex offender list until age 43. He told MTV that he was kicked out of college, can't find work, and he can't live with his father because his dad lives near a school.

CONSEQUENCES OF SEXTING

One interesting set of findings from that 2008 Cox study is that 90% of youth who admitted that they "sent a sext" reported that nothing bad happened as a result. Two percent said that they got in trouble after the photo was forwarded to an "authority figure"; only 1% said the photo was posted online; 2% said the person they sent the photo to made fun of them; 2% said the photo was forwarded to someone they didn't want to see it; and 4% said the person they sent the photo to threatened to send it to someone else. The study found that 14% of "sexters" said they were caught by parents (9%), a teacher (1%), another authority figure (3%) or someone else (3%)

Though most incidents of sexting never make it to legal authorities and, even when they do, most police and prosecutors are using their discretion to deal with the cases without resorting to criminal prosecution, there have been some cases where minors have been arrested, tried and convicted of manufacturing, possessing and/or distributing illegal child pornography. Some States are addressing the issue by decriminalizing the voluntary taking, possession and consensual sharing of sexual or nude images between minors. Recently, some courts have addressed the use of child pornography and sex offender laws in sexting cases, chastising over-zealous prosecutorial actions.

The National Center for Missing & Exploited Children's Policy Statement on Sexting[20] provides advice to law enforcement on what is and is not sexting and how to approach individual cases. "NCMEC," according to the policy, "does not believe that a blanket policy of charging all youth with juvenile or criminal violations will remedy the problem of sexting."

The Youth Online Safety Working Group (YOSWG) which consists of several law enforcement, child protection and education organizations and agencies, has developed an "Interdisciplinary Response to Youth Sexting" for educational professionals and law enforcement. The document recommends, among other things, that authorities "recognize possible causes of sexting within schools by examining school climate and any underlying behavioral issues" and that they "use discretion when

18 "Sexting Shockingly Common Among Teens" at CBSNews.com (http://www.cbsnews.com/stories/2009/01/15/national/main4723161.shtml)

19 MTV Documentary: *A Thin Line* (http://www.athinline.org/)

20 The National Center for Missing & Exploited Children: Policy Statement on Sexting (http://www.missingkids.com/missingkids/servlet/NewsEventServlet?LanguageCountry=en_US&PageId=4130)

determining legal actions." YOSWG is also recommending prevention education programs for educators and law enforcement and is encouraging a "team approach" to "combat the problem of sexting."[21]

INAPPROPRIATE CONTENT

The report of our Sub-Committee on Parental Controls Technologies deals extensively with the issue of inappropriate content, but there is also an educational component to this issue. In addition to all of the child-friendly material online, there are some websites that contain material that most would agree can be harmful or at least disturbing to children.

These include sites that depict sexual content as well as those that encourage hate speech, violence or unsafe activities such as drinking, drug use or eating disorders. With some exceptions (such as child pornography, obscenity and sites that advocate violence against individuals), this material is constitutionally protected and any efforts to keep children from seeing it must be balanced with the rights of adults to produce and consume such material.

At its September meeting, the Working Group heard from Jessica Gonzales of the National Hispanic Media Coalition and Steve Sheinberg from the Anti-Defamation League about the impact of hate content on youth. Ms. Gonzales warned of the harmful impact of online "speech that induces encourages or otherwise legitimizes violence against particular groups of people, that … truly crosses the line or dances very close to the line of unprotected speech." Mr. Sheinberg agreed but observed (speaking for the ADL) that "We believe that the best antidote to hate, to hate speech is more speech – is good speech."

While, in most cases, there is nothing government can do to take down such material, there are ways that government can help parents in their own efforts to both shield their children from such material and help their children more effectively deal with it when they do encounter it. This includes education on the availability and use of parental control tools and encouraging instruction in critical thinking and media literacy – helping children understand how to make good decisions when selecting material for consumption and processing material that they see. It also includes helping parents better understand the actual impact of inappropriate material, which varies greatly based on the material itself, the maturity of the child and the extent of exposure, for example occasional exposure versus obsessive interest in certain types of sexual content.

OTHER RISKS

There are other risks children face online. In his introduction to "A Broadband Plan for Children and Families"[22] this March, Federal Communications Commission Chairman Julius Genachowski talked about "Harmful Websites," pointing out that "35% of eating disorder patients visit pro-anorexia websites." He also discussed distracted driving, citing data that "a quarter of U.S. teens with cell phones say they have texted while driving," an activity that can clearly lead to death or serious injury. He also discussed "Inappropriate Advertising" that exposes young people to potentially unhealthy or inappropriate messages such as ads for male enhancement drugs or sugary foods. These, along with access to online pornography, hate sites, and many other problem areas related to the Information Age are a constant challenge for young people.

21 "Interdisciplinary Response to Youths Sexting" (http://docs.google.com/viewer?url=http://www.netsmartz.org/downloads/special/InterRespYouthSexting.pdf&pli=1)

22 FCC's Broadband Plan for Children and Families (http://hraunfoss.fcc.gov/edocs_public/attachmatch/DOC-296829A1.pdf)

SECURITY RISKS AND IDENTITY THEFT

Young people, along with the rest of us, are also exposed to spam, malicious software, phishing attacks and other modern-day scourges that can invade their privacy, jeopardize the security of their computer and other devices and, in some cases, lead to financial loss, identity theft and damaged reputations. Contrary to what some people might think, children and teens are vulnerable to identity theft[23] because their typically squeaky clean credit histories make them valuable targets. Young people need to understand how to protect themselves from online criminals and hackers not only by knowing how to use protective tools like security software but by understanding "social engineering" – how bad actors can manipulate even savvy Net users into disclosing confidential information. Helping young people learn to protect themselves and their devices from criminals and deceptive social engineering practices can itself be a lesson in media literacy and online safety.

There is also the risk that a young person might do something that gets him or her in trouble with school authorities or the law. Regardless of other consequences, there can be legal or academic sanctions for a wide range of activities, including being depicted online drinking alcohol or illegally using drugs, being involved in gang activity, sexting, cyberbullying, using cell phones to cheat on exams and illegally downloading music and other media.

Further, there is the risk of over-use or obsessive use of technology that interferes with a young person's other activities, including exercise, schoolwork, family time and in-person interaction with peers. Young people need to learn that everything has its time and place and that the inappropriate use of technology (such as texting at the dinner table, or updating their social-networking profile when they should be doing homework, sleeping, or playing outside) needs to be avoided. And adults need to think of how they are modeling this behavior in front of their own children and other youth.

There is the risk of loss of reputation. What we post online can live online forever and what may seem funny or appropriate at the time could turn out to be embarrassing later on. Youth need to understand how to set the privacy features of the services they use and understand that even with these tools in place, it's possible for anything that's posted online (even if they think it's only for their friends) to be copied, stored or forwarded.

Finally, there is the risk of young people being denied access to technology and social media for a host of reasons ranging from financial obstacles, geographic isolation and attitudes and fears that cause adults to deny them access either at home or at school. For some youth, this could be the greatest risk of all because lack of access to technology correlates with lack of access to educational and job opportunities, health care information and participation in modern society.

WHAT WE KNOW ABOUT RISK PREVENTION

It's beyond the scope of this report to go into great detail about all youth risk prevention but there are some things we do know from researchers and risk-prevention practitioners. The first is that a "fear-based approach" is not an effective strategy. Referring to "scare tactics" used in alcohol education projects, sociologist H. Wesley Perkins told the Yale Alumni Magazine that "traditional strategies have not changed behavior one percent."[24]

23 National Crime Prevention Council: "Protecting Teens from Identity Theft" (http://www.ncpc.org/programs/teens-crime-and-the-community/publications-1/preventing-theft/adult_teen%20id%20theft.pdf)

24 Yale Alumni Magazine: "A Closer Look at Alcohol" (http://www.yalealumnimagazine.com/issues/01_05/alcohol.html)

In 1986, Perkins and Alan Berkowitz published a paper which concluded that providing students with evidence that excessive drinking is not a "norm" among their peers had a better outcome than trying to scare them. The norms approach is also a more effective way to curtail bullying. In a paper presented at the 2008 National Conference on the Social Norms Approach, Perkins and David Craig found that "while bullying is substantial, it is not the norm. The most common (and erroneous) perception, however, is that the majority engage in and support such behavior." The researchers found that the "perceptions of bullying behaviors are highly predictive of personal bullying behavior," but that the "norm is not to bully, but only a minority know it."[25]

Based on this research, the commonly repeated mantra that cyberbullying is reaching "epidemic proportions" is counterproductive. Perhaps a better message is to remind youth that most kids don't bully other kids (cyber or otherwise) and that those who do are exhibiting abnormal behavior. Craig and Perkins presented a series of posters used at middle schools with messages like "80% of Crystal Lake 6-8th grade students say students should not treat each other in a mean way, call others hurtful names or spread unkind stories about other students."

The research also shows that most youth are remarkably capable of dealing with Internet problems. A 2008 study on the impact of parenting style and adolescent use of MySpace found that "For all Internet problems, the vast majority of MySpace teens either had appropriate reactions (telling the person to stop, blocking the person from the MySpace page, removing themselves from the situation by logging off, reporting the incident to an adult or to MySpace authorities) or ignored the behavior."[26]

The study also found that "parenting styles were strongly related to adolescent MySpace experiences, behaviors and attitudes." Parents who engage with their children's use of media in an "authoritative" manner (exerting authority while remaining responsive to their children) were more effective than those who were "authoritarian" or "neglectful."

Further, there is some evidence that social networks can be protective in helping to shape and reinforce positive norms. In an online video[27] describing the book *Connected: The Surprising Power of Social Networks and How they Shape Our Lives*, co-author James Fowler observes how social networks (real world or online) can influence behavior. "If your friend's friend's friend becomes obese it increases the likelihood of your becoming obese." But it can also have a positive effect. "If your friend's friend's friend quits smoking then it will also have an impact on whether you're going to quit smoking."

Based on data from the Framingham Heart Study, the two authors found "an individual's chance of becoming obese increased 57% if someone named as a friend became obese in the same time interval," according to an article in the January 23, 2009 edition of *Science*[28].

The same principle can apply to young people online. When he addressed the September, 2009 OSTWG meeting, USC media Professor Henry Jenkins pointed out how young people in online communities tend to have a positive impact on each others' behavior through social norming. "Some of the fan cultures that I've studied," he told the OSTWG meeting, "have incredibly ingrained ethics, ways of teaching, mutual support systems."

---

25 "Assessing Bullying in New Jersey Secondary Schools" http://www.youthhealthsafety.org/BullyNJweb.pdf

26 "The Association of Parenting Style and Child Age with Parental Limit Setting and Adolescent MySpace Behavior," by Dr. Larry Rosen, in *Journal of Applied Juvenile Psychology*, November-December 2008

27 *Connected: The Surprising Power of Social Networks and How They Shape Our Lives,* by Drs. Nicholas Christakis and James Fowler, Little, Brown and Company, September 2009 (http://www.connectedthebook.com/)

28 "Friendship as a Health Factor" in Science (http://jhfowler.ucsd.edu/science_friendship_as_a_health_factor.pdf)

Jenkins also talked about work he has done with the MacArthur Foundation that found that "kids who engage in participatory practices online also increase opportunities for civic engagement at about the same rate as being on the school newspaper, being on the debate team – the same sort of activities that have traditionally been enshrined as the birthplace of civic skills."

In a 2009 video[29] for the Carnegie Foundation for the Advancement of Teaching, USC visiting scholar and former Xerox PARC director John Seely Brown said it this way: "We have to get kids to play with knowledge." Kids have to be able to "create, reflect and share," and "in that sharing you start to build a whole new kind of culture because you begin to get a kind of peer-based learning … where the kids can learn from each other as much as from the mentor or the authority figure."

So, based on the research and the opinions of several experts, one of the biggest risks to children may be adults who try to shut down the informal learning involved in their use of Internet technologies at home or school.

PREVENTION NEEDS TO BE TAILORED TO RISK

Different kids are susceptible to different risks and need different approaches to prevention and intervention. In 2009, the Internet Safety Technical Task Force concluded that not all youth are equally at risk. Youth with offline high risk profiles tend to be similarly at risk online.

This point was made very clearly at the September 2009 OSTWG meeting by Dr. Patricia Agatston, a counselor and prevention specialist with the Cobb County (GA) School District's Prevention Intervention Center. She is also a trainer, technical assistant consultant for the Olweus Bullying Prevention Program, and co-author of *Cyber Bullying: Bullying in the Digital Age* and cyberbullying curricula for grades 3-5 and 6-12.

At the OSTWG meeting, Dr. Agatston talked about how the Primary, Secondary and Tertiary models that are used in health-related prevention work need to be applied to youth online risk.

- **Primary** prevention includes the basic skills, knowledge and behavioral information that all online kids need. Because most kids don't take extraordinary risks, primary prevention is what should be used for the vast majority of youth.
- **Secondary** prevention applies to kids who are at somewhat higher risk such as kids who live in gang-infested neighborhoods or who have exhibited some early behaviors that are likely to correlate to risk
- **Tertiary** prevention and intervention is used with what are commonly called "high risk youth" who not only need special messaging but, likely, professional intervention with a psychologist or, in extreme cases, in a hospital setting.

Although this framework has been fully accepted by the Centers for Disease Control and other health agencies for prevention of physical diseases and other risks, such as drug and alcohol abuse, it's rarely applied to Internet safety messages or bullying. But Dr. Agatston assured the Working Group that it can apply to online behaviors. "Some of the things that we look at with primary prevention are: What is it that's going to help kids be in a safe environment and grow up safe and have the skills and education

29 "Tinkering as a Mode of Knowledge Product" a video interview with John Seely Brown (http://vodpod.com/watch/1390547-john-seely-brown-tinkering-as-a-mode-of-knowledge-production?pod=cathyinoz)

they need to make healthy choices?" While a lot of primary prevention does occur at school, it also takes place in the community, she told the group. "There are certainly things that are already going on right now where it fits, where we could infuse media literacy, digital citizenship, and online safety in all the appropriate areas in the school and in the classroom because that's where kids spend most of their time, obviously, but primary prevention also takes place in the community."

Also, as we have shown above, it is effective to involve peers, not just adults, in risk prevention and education. Social-norm education and peer-mentoring programs have had proven effectiveness in reducing youth risk. For example, Finland has a 38-year-old "peer-support"[30] program that operates in 90% of its schools. Now including Net-safety lessons, the program involves more than 10,000 middle-school-level "peer students" or mentors working with primary school students. The program – which was featured at the European Commission's 2009 Safer Internet Forum – is designed to "increase social responsibility and secure a safe, enjoyable and supportive school year for all," according to the Mannerheim League for Child Welfare in Finland and speaks to the view of U.S. psychologists and risk-prevention specialists that, where schools are concerned, the most likely solution to cyberbullying is a "whole school" approach.[31]

ONLINE RISK CORRELATES WITH OFFLINE RISK

Dr. Agatston reinforced an important finding by the Berkman Online Safety Technical Task Force, which observed, "Minors who are most at risk in the offline world continue to be most at risk online." The Berkman report cited research that found, "Female adolescents ages 14–17 receive the vast majority of solicitations (Wolak et al. 2006). Gender and age are not the only salient factor. Those experiencing difficulties offline, such as physical and sexual abuse, and those with other psychosocial problems are most at risk online (Mitchell, et al. 2007)."

Many of today's Internet safety messages fail to take into consideration the fact that not all youth are equally at risk. The problem with this one-size approach is that the messages are not getting through to the very youth most in need of intervention. It is analogous to inoculating the entire population for a rare disease that most people are very unlikely to get while at the same time failing to inoculate the population that's most at risk.

HOW YOUTH ARE USING SOCIAL MEDIA

In addition to understanding the risks, it's important to understand how young people use social media and technology. In *Living and Learning with New Media: Summary of Findings from the Digital Youth Project,* researchers summarized the findings of the MacArthur Foundation's five-year, $50 million digital media and learning initiative to "help determine how digital media are changing the way young people learn, play, socialize, and participate in civic life." [32]

The researchers found that, "Most youth use online networks to extend the friendships that they navigate in the familiar contexts of school, religious organizations, sports, and other local activities" and that "a smaller number of youth also use the online world to explore interests and find information that goes beyond what they have access to at school or in their local community." Both these "*friendship-driven*" and "*interest-driven* networks" amount to informal learning environments

30 "Peer Support in Schools" from the Mannerheim League for Child Welfare (http://www.mll.fi/en/peer_support_in_schools/)

31 "Bullies: They can be stopped, but it takes a village," by Yale University Prof. Alan Yazdin and Boston College Prof. Carlo Rotella (http://www.slate.com/id/2223976)

32 "Living and Learning with New Media: Summary of Findings from the Digital Youth Project" (http://digitalyouth.ischool.berkeley.edu/report)

where "youth are picking up basic social and technological skills they need to fully participate in contemporary society." The researchers argue that "erecting barriers to participation deprives teens of access to these forms of learning" and that "youth could benefit from educators being more open to forms of experimentation and social exploration that are generally not characteristic of educational institutions."

The implications of the MacArthur research are profound in that they demonstrate how young people have taken it upon themselves to create their own learning environments that, for the most part, are not supported, endorsed or even acknowledged by the formal learning environment called school.

"Unfortunately, many children are not learning effective digital or media literacy skills at home or at school," FCC Chairman said in his presentation of the "Digital Opportunity: A Broadband Plan for Children and Families." In fact, many parents and teachers tell us that they don't sufficiently understand digital technology, much less know how to teach kids about how use it effectively."

Tech educator and author Will Richardson calls it "the decoupling of education and school."[33] And the MacArthur researchers ask, "What would it mean to really exploit the potential of the learning opportunities available through online resources and networks?"

The question is not rhetorical nor is it unrelated to our topic of youth online safety. Now that so much media has a social or behavioral component, learning constructive behavior is part of learning the effective, enriching use of media. But schools' liability fears and extensive filtering, in some cases, causes educators to abdicate their long-held responsibility of guiding and enriching young people's experience with current media.

New-media literacy and citizenship are not just academically enriching, they are also protective in a social-media environment. A 2007 study in Archives of Pediatrics & Adolescent Medicine found that "youth who engage in online aggressive behavior ... are more than twice as likely to report online interpersonal victimization" (Ybarra, et al[34]). Unless new media are used in schools and within families, youth are on their own in figuring out the ethics, social norms, and civil behaviors that enable good citizenship in the online part of their media use and lives. We are not suggesting that schools allow kids to update social network profiles in class but rather that schools find ways to incorporate educational social-technology tools in the classroom to enhance learning and provide pre-K-12 educators with an opportunity to, in the process of teaching regular subjects, teach the constructive, mindful use of social media enabled by digital citizenship and new-media-literacy training – using the media and technologies familiar and compelling to students.

By way of an analogy, imagine if there were no organized sports programs in schools or communities. Kids would still play "ball" in the streets, their backyards and in parks but they would have no formal training in rules, the ethics of fair play or appropriate ways to interact with teammates and opponents. Kids would make up the rules as they go along and would be deprived of all they learn now from coaches, PE teachers and other adults who mentor young athletes. In many ways, that's exactly what is happening with teens' use of social media. They're playing, but there are very few coaches to help them avoid unsportsmanlike conduct and learn to slide home without skinning their knees.

33 "The Decoupling of Education and School: Where do We Begin? (http://weblogg-ed.com/2010/my-educon-conversation/)

34 "Online Behavior of youth who engage in self-harm provides clues for preventive intervention" (http://www.unh.edu/ccrc/pdf/CV160.pdf)

THE STATE OF NET-SAFETY EDUCATION IN THE UNITED STATES

INDUSTRY EFFORTS IN NET-SAFETY EDUCATION

In his testimony at our September meeting, Family Online Safety Institute CEO Stephen Balkam referred to industry's role as "a multi-million dollar effort" for which "virtually all of the major players have set aside not just funds and resources but personnel and time and energy to try and get this issue right." (FOSI is a Washington-based international Internet safety organization whose members include Internet, social networking and telecommunications companies.)

In addition to efforts in developing tools and education programs, Balkam reminded the Working Group about "the rules that companies develop, their terms of service, which are a critically important part of safety." Balkam pointed out how some sites put messaging exactly where it needs to be. "One of the things I found fascinating in the discussion we just had was the remark that I got a safety message as I was leaving MySpace, or when I was using Hotmail, I was told that I was going to go to an insecure site."

He also pointed out that "there has been a significant move away from a rather fear-based approach and [toward] using more ... research of actual harm."

Balkam said there are still some challenges. "Some companies are rather disconnected from each other, sometimes acting both in isolation but also acting in a vacuum. We [companies] don't have a coherent set of meta-messages from government, a 'Smokey the Bear' type of message or the seat belt campaigns upon which to anchor their own messages and tools." And, in response to a question, he noted that there is sometimes a disconnect between a company's messaging and the people who should be delivering those messages. He gave an example: "We live in Rockville [Md.], and in the town square, there are about four or five different cell phone shops. I just did a very random survey. I walked into each one and virtually all of [the people working in the stores] weren't aware that they had safety controls on their phones."

All major social network sites offer some type of user education, and many provide financial support for non-profit organizations to extend that message beyond users to the general public. Some have brought cybersafety experts together to advise them or provide content for their sites and networks. This group does not have the resources to chronicle what every company is doing, but here are some examples from major social-network and Internet companies.

See Addendum B for details on how several companies are dealing with Internet safety education.

INTERNET-SAFETY EDUCATION FROM NONPROFIT ORGANIZATIONS

The U.S. is home to numerous non-profit organizations and other operators of websites and blogs with online safety educational resources. Addendum A at the end of this section lists just a sample of them. When you count the numerous local and state resources, it is much larger. Some of these groups have paid professional staff, others rely on volunteers and some use a combination of staff and volunteers. Funding for these groups varies from none at all to millions of dollars annually. Sources can include the federal government as well as states, counties, municipalities and school districts as well as foundations, corporate giving programs and donations from the public along with fees for services and products.

Collectively, these organizations reach tens of millions of youth and parents and educators annually with such resources as:

Safety tips and guides	Videos & cartoons	In-school assemblies and training
Safety curriculum, classroom activities and workbooks	Online interactive forums	Reporting mechanisms to resolve safety and privacy related problems
Resources about parental control tools	Safety related games	Mobile phone apps
Presentations at parent nights & community events	Law enforcement training and professional development	Outreach to seniors and caregivers
Brochures, handouts and books	Youth organized events and initiatives	Comic books
Public service announcements (print, TV, radio, online)	Websites, e-newsletters and online widgets	

Topics covered by these organizations include

Cyberbullying & harassment	Hate speech	Violence
Digital citizenship and ethics	Digital literacy and critical thinking	Cell phone safety
Online pornography	Predators	Media literacy
Distracted driving including texting while driving	Obsessive use of technology	Virtual world safety
Cyber security	Password protection	Social networking skills
Online gambling risks	Scams, fraud and consumer protection	Digital dating abuse / sexting
Copyright and piracy	Security and privacy	Cyberwellness and balance
Social engineering awareness.	Online/Digital Reputation	Gaming Safety
Video game ratings, parental controls and playing games online		

Online-safety education at school

Almost all educators agree that schools have a role to play when it comes to Internet safety. A February, 2010 survey[35] conducted by Zogby International for the National Cyber Security Alliance (NCSA) and funded by Microsoft, found that 100% of technology coordinators, 97% of school administrators and 95% of teachers agreed that "Cyberethics, Cybersafety and Cybersecurity curriculum should be taught in schools."

There is less agreement, however, as to whether districts are doing it right, with 84% of administrators, 83% of technology coordinators and 65% of teachers either somewhat or strongly agreeing that their district does an "adequate job."

Of the administrators surveyed, 95% said their schools use filters, 91% require students and parents to read an acceptable use policy or student code of conduct and 86% require students to sign an appropriate use contract. More than nine out of ten (91%) say they block social network sites. The *Children's Internet Protection Act* of 2000 requires schools and libraries receiving federal E-Rate funds to implement "filtering," a technology protection measure which blocks visual depictions of obscenity, child pornography or anything else harmful to minors. According to the National Conference on State Legislatures, 21 states also have Internet filtering laws to block similar material.[36]

As for filtering as a safety measure, there is a growing discussion about its use and effectiveness in the US and overseas. In the UK, government education watchdog Ofsted released a report this past February that rated 5 of 37 schools "outstanding" in online-safety provisions. The five "all used 'managed' systems to help pupils to become safe and responsible users of new technologies. 'Managed' systems have fewer inaccessible sites than 'locked down' systems and so require pupils to take responsibility themselves for using new technologies safely," Ofsted reported. The schools that used the stricter "locked down" filtering systems "kept their pupils safe while in school," the agency added, but "such systems were less effective in helping them to learn how to use new technologies safely."

The NCSA study found interesting discrepancies between the way administrators feel about their efforts and how teachers feel. For example, 66% of administrators said they were prepared (29%) or very well prepared (37%) with strategies to protect against malicious software, phishing, and other scams. But only 40% of teachers agreed the school was prepared. The same was true with cyberbullying, where 75% of administrators thought the school was prepared, compared to 50% of teachers thinking so. With sexting, it was 66% compared to 48%. Perhaps the most glaring discrepancy was the answer to "who is primarily responsible for teaching children to use computers safety and security?" Seventy-two percent of teachers said "parents," but only 42% of administrators agreed; 51% of administrators said "teachers," while only 23% of teachers said "teachers." It seems that teachers and administrators have a different notion of what does and should go on in their schools when it comes to Internet safety training.

Differing perceptions of students and parents

The results of a massive study of students, parents and educators by Project Tomorrow[37] are even more

35 "The State of Cyberethics, Cybersafety, and Cybersecurity Curriculum in the US": Survey (http://www.staysafeonline.org/content/ncsa%E2%80%99s-national-k-12-studies)

36 "Children and the Internet: Laws Related to Filtering, Blocking and Usage Policies in Schools and Libraries" (http://www.ncsl.org/issuesresearch/telecommunicationsinformationtechnology/stateinternetfilteringlaws/tabid/13491/default.aspx)

37 Project Tomorrow's "Speak Up" surveys of school administrators, teachers, students, and parents (http://www.tomorrow.

revealing. For the 2009 Speak-Up survey, researchers interviewed 299,677 students, 38,642 educators and 26,312 parents in 5,757 school districts across the country.

When asked "what is the best way for you to learn about being safe on the Internet?" only 12% of all middle and high school students, but a notable 41% of parents said "by using technology as part of my regular classes."

The highest response was from "parents and other family members," but even here there was a major discrepancy between students and parents: 53% of students in grades 3-5, 30% of middle-schoolers and 22% of high school students agreed that family members were the best source of safety education, while 61% of parents responded with "me" as the best source.

Forty-one percent of parents thought that an Internet safety class is the best method for teaching safety, but only 8% of middle-school students and 6% of high-schoolers agreed – although nearly a quarter (24%) of students in grades 3-5 agreed.

More than one in five third-to-fifth-graders (21%), 19% of high school students and 11% of middle schoolers selected "learn on my own just by using technology," yet only 4% of parents agreed.

The survey not only reveals an enormous perception gap between parents and students but calls into question some of the most commonly used strategies for teaching Internet education. And despite the amount of time they spend in school, students still selected parents and family members as the most effective way to learn how to be safe online, though the older the kids were, the less likely they were to agree with that statement.

Is blocking social media the right approach?

Although they weren't asked this question, we suspect that most of the 91% of administrators who told the NCSA researchers that they block social network sites, are doing so because they believe it is in the best interest of their students, but there is a growing consensus among Internet-safety experts that blocking social media might actually have a negative effect on student safety.

In her testimony before the September 2009 OSTWG meeting, Nancy Willard of the Center for Safe & Responsible Internet Use expressed concern that schools that block access to Web 2.0 technologies may be missing an opportunity to teach Net safety. "There are some significant barriers in school to get to where we need to be because, in order to teach Internet safety in school, we have to teach it in context, and if we have these major barriers of getting Web 2.0 technologies into schools, then we're not going to be able to teach these skills in the context of learning," she said.

Besides, said educator Mike Donlin at the same meeting, students "can get around the firewalls, but they don't need to. They have [the Internet on cellphones] in their pockets; they can do what they want to do." Donlin is a senior program consultant for Seattle Public Schools, the developer of the district's award-winning cyberbullying curriculum, and recipient of the 2008 Spirit of Online Safety Leadership Award from Qwest Communications and the National Center for Missing & Exploited Children.

Donlin pointed out that most teachers are "digital immigrants" trying to impart knowledge to the students who are "digital natives." The problem is that "we really don't live in the same worlds.… There's a lack of understanding of the kinds of things that happen, the way and the speed in which

org/speakup/speakup_reports.html)

they happen and the ease with which things happen." NCSA's research backs this up, as 76% of teachers surveyed reported less than 6 hours of professional development on cyberethics, cybersafety, and cybersecurity

An Internet search for "bypass school Internet filters" returns thousands of results. While there are some filtering companies which claim that their software is more kid-proof than others, the bottom line is that a lot of young people know workarounds to filters. Schools could invest more precious resources on tighter filters in a never-ending battle to outsmart their own students, but is that really the way schools should be spending their resources?

The solution, in part, said Donlin, is professional development. "If we have the mandates to teach, to educate minors about online safety, online behavior, it doesn't just happen. We have to take the time to train the teachers, to train the educators and the administrators and the counselors and the professionals who are going to be working with the kids."

And it takes a concerted effort. "Everybody has to be involved. Administrators have to know what they're doing, what they're seeing, how to deal with things. Counselors have to know how to counsel kids, especially the kids who are ... at higher risk because of being harassed or because of things happening to them. We have to include law enforcement. We have to include the industry, we have to include parents, and we have to include the kids themselves," he said.

In a follow-up email, Donlin pointed out that "Much of the [Internet safety] conversation is being led by non-educators, people outside the K-12 world. Others are making 'decisions' which we will have to implement. Not all those decisions – or materials – are educationally appropriate.… K-12 has to be at the table from the get-go. We cannot be handed 'stuff' and told to teach the kids, as we are now mandated to do."

School-based Net-safety curricula

There are numerous Internet safety curricula being used in school districts around the United States and more on the way. Some come from non-profit organizations, some from businesses and publishers and others have been developed by school districts and even individual teachers.

Although individual programs have been evaluated by developers, users and, in some cases, funders, there has yet to be a large-scale national study to look at the accuracy and effectiveness of these programs. And the lack of a coherent evaluation causes David Finkelhor, director of the Crimes Against Children Research Center, to question whether it makes sense for us "to be going to scale with education programs unless they have been evaluated and found to be successful." In an interview for this report, Dr. Finkelhor, who has spent years researching youth risk, said that current programs are typically "based on hunches that people have about messages that young people should be getting." He also questioned whether kids are changing their behavior based on those messages. Finkelhor added that it's important to understand "what the dangers are, who the at-risk individuals are, what the dynamics of dangers are and also what kinds of messages actually prevent those kinds of situations."

Finkelhor questions "whether it makes sense to do cybersafety education independent of a more comprehensive safety and socio-emotional development program." The "skills that we're talking about and trying to develop in terms of making judgments about dangerous situations, not being

mean towards other people, reporting things to or discussing things with adults and parents, taking responsibility for your own behavior and things like that ... these apply in all areas."

Finkelhor joins other youth-risk experts in saying that "fear-based instruction isn't all that effective, that kids need opportunities to role-play situations in order to adapt, to develop new skills. We've learned something about motivation, that they need to sort of feel they have some kind of a stake in it."

Finkelhor also agrees that we need to rethink the "one-size-fits-all" approach to online-safety education but admits that that approach is "less expensive and is also less stigmatizing**."** He added: "We understand conceptually that kids who are at high risk may need additional or supplementary or different kinds of interventions. In some cases it may be at the level of needing some kind of real psychotherapy to deal with problems that are behind their maladaptive behavior, so if they have anxiety or depression or some underlying mental health issues." Again, he's referring to real-world risk as much as online risk.

The relative lack of information on which strategies are actually effective in increasing youth online safety and responsibility has prompted the National Institute of Justice to fund the CACRC to conduct a study on the effectiveness of youth Internet safety programs. The project, which will likely complete its work around December 2011, will rate and compare the content of four prominent youth Internet safety curricula (Netsmartz, i-SAFE, Web Wise Kids, and the Internet Keep Safe Coalition). The CACRC will also "conduct a process evaluation that will document and evaluate the procedures, audiences and contexts of Internet-safety education programs delivered by ICAC Task Forces and "provide recommendations and piloted materials to ICAC Task Forces to enhance prevention efforts and facilitate future outcome evaluation research."

The project will develop an evaluation toolkit with piloted outcome measures for use in future program monitoring and outcome evaluation efforts as well as an Internet Safety Prevention Clearinghouse or "portal for the placement of Internet prevention education materials and relevant research data."

THE NEED FOR EVALUATION OF INTERNET-SAFETY PROGRAMS

When looking at the effectiveness of any training or curriculum, it's important to consider both whether it is effective in teaching what it aims to teach and whether what it is trying to teach is relevant, accurate and helpful.

For example, much of our Internet-safety education has been focused on helping kids protect themselves from Internet predators, yet, as indicated above, the research shows that the overwhelming majority of students are very unlikely to be harmed by adults they first encounter online. Some will argue that that fact doesn't matter because it's "better to be safe than sorry" but, again, there is reason to question that assumption, based on what we know about the overall lack of effectiveness of "scare tactics," especially when what adults are saying doesn't resonate with young people's own experiences. There is also the risk of youth being "turned off" to authorities if they hear messages they believe to be incorrect. Other risks of scare tactics include focusing on the wrong messages to the detriment of more likely risks and, finally, the risk that fear, rather than motivating, can actually inhibit action.

For example, a 2005 George Washington University study[38] to evaluate the effectiveness of an Internet safety education program found that prior to receiving the training, 25% of the students were unsure

38 "Evaluation of the Effectiveness of the NetSmartz Program: A Study of Maine Public Schools" (http://www.netsmartz.org/pdf/gw_evaluation.pdf

or believed it was safe to post their picture on the Internet but after the training, 96% felt it was unsafe. The same study found that 20% of kids thought it was safe to reveal their real name online but after the training 98% felt that disclosing their real name on the Internet was dangerous.

Clearly that training was effective in changing student's understanding of risk but the larger question is whether that "knowledge" was based on actual risk. When this training was conducted, there was widespread belief among Internet safety advocates and educators that the posting of pictures and personal information was dangerous, but a study conducted by the Crimes Against Children Research Center and summarized in the February 2007 *Archives of Pediatrics & Adolescent Medicine*[39] shows that these particular behaviors don't necessarily correlate to an increase in victimization, whereas "engaging in a pattern of different kinds of online risky behaviors" such as "talking about sex online with unknown people" does correlate with increased risk."

Another set of issues is whether the training is effective and how "effectiveness" Is defined. For example, a 2006 independent evaluation[40] of another training program found that students who had been through the program had "positive and significant" improvement in knowledge, indicating that the program had been effective in getting children to learn about what the program considered to be risky behaviors. However, the study also found that the program didn't significantly change students' behavior. One reason for that was that, even before the program, the majority of students were already using the Internet safely. The "low levels of risky behavior measured at baseline" prompted the researchers to suggest that programs like these "be targeted at youth who have been identified as at-risk for inappropriate behavior or who have been caught engaging in high-risk behavior," adding that "this recommendation does not suggest, however, that the program be taught only to high-risk youth."

The issue of cause and effect also comes up in policy recommendations. For years a number of state attorneys general called upon social network sites to use technology to verify the age of their users, yet a thorough evaluation of the necessity and effectiveness of this technology by the Berkman Center's ISTTF found that age verification is not only not effective but not necessarily advisable. There was some evidence presented to the Task Force that it might actually endanger youth by keeping adult guidance or supervision out of online spaces where peer-on-peer harassment or cyberbullying could occur.

Internet-safety education from the Federal Government

There have been a number of federal resources aimed at Internet safety education going back at least to the mid-90s. Several agencies, including the Justice Department, Federal Trade Commission, the Department of Education, the Department of Homeland Security, FBI and others have, over the years, provided a variety of educational resources online, in printed form, on the Web, and through in-person presentations. In 1997, for example, the Department of Education created the Parents Guide to the Internet,[41] which included a section on "Tips for Safe Traveling" on what the guide referred to at the time as "the Information Superhighway." In April 2000, the Federal Trade Commission launched a "KidzPrivacy" Web site tied to the start of COPPA enforcement. The FBI posted its own "A Parent's Guide to Internet Safety" that warned parents about the dangers of predators and in 2008, the Department of Justice's Project Safe Child launched a public awareness campaign that featured public service

39 "Internet Prevention Messages: Targeting the Right Online Behaviors" in Archives of Pediatrics and Adolescent Medicine, February 2007 (http://archpedi.ama-assn.org/cgi/content/full/161/2/138)

40 *I-Safe Evaluation*, Susan Chibnall, Madeleine Wallace, Christine Leicht, Lisa Lungihofer, April 2006, ICF Consulting Company (http://go2.wordpress.com/?id=725X1342&site=csriu.wordpress.com&url=http%3A%2F%2Fwww.ncjrs.gov%2Fpdffiles1%2Fnij%2Fgrants%2F213715.pdf)

41 US Department of Education: *Parents Guide to the Internet* (http://www2.ed.gov/pubs/parents/internet/index.html)

announcements aimed at children, parents and "potential predators." These PSAs were part of a $2.5 million allocation to fund a national public education and awareness program through partners including the Self Reliance Foundation, Hispanic Communications Network, INOBTR (I Know Better) and the Internet Keep Safe Coalition (iKeepSafe).[42]

Another major federal effort has been the work of Internet Crimes Against Children Task Forces (ICAC). Although their role is primarily in the area of law enforcement, ICAC officers have made themselves available to teach Internet safety to students and parents in communities throughout the country. The 61 ICAC's Task Forces are operated out of local, state and regional law enforcement agencies with support from the Department of Justice.

An ICAC's name says a lot about its mission. It focuses on crimes against children. ICAC officers are well versed on issues such as online enticement and child pornography and not necessarily equipped to handle other areas of youth risk, although some ICAC officers do talk about cyberbullying and other youth-on-youth risks and self-destructive behavior. Still, the emphasis tends to be on the legal and criminal risks which, the expertise of the presenters, and – while an entirely appropriate focus for law enforcement, these are not the risks that research shows students most commonly face online.

Although the Justice Department, with its focus on law enforcement, is probably the most active participant in Internet safety, there are other federal agencies that provide research and educational materials.

The Centers for Disease Control, for example, in 2008 published *Electronic Media and Youth Violence: A CDC Issue Brief for Educators and Caregivers,*[43] focusing on cyberbullying.

The Substance Abuse and Mental Health Services Administration hosted a summit on suicide prevention in 2009 with NGOs in the risk-prevention and Internet-safety fields and presented a white paper on expanding prevention, intervention and postvention (i.e., bereavement support for friends, family and classmates following a suicide) through social media as an effective means for reaching out to and educating youth in crisis. That work continues with the launch in March of ReachOut.com for teens, supported by a nationwide public-service media campaign, "We Can Help Us," all produced in cooperation with the Inspire USA Foundation and the Ad Council. We recognize this important work in this report, not only because SAMHSA will use the Internet to deliver its materials but because issues of youth suicide, eating disorders and self-harm are now impossible to separate from use of the Internet. The Internet can be used to encourage self-destructive behavior but it can also be used to flag, intervene in and prevent such behavior. Young people are alive today because a "friend" (or perhaps a "stranger") recognized their distress signs online and did something to help.

One of the more innovative Federal approaches to Internet safety comes from a coalition of agencies under the umbrella of OnGuardOnline.gov. Operated by the Federal Trade Commission, the project enjoys "significant contributions" from a wide range of partners including the Department of Justice, Department of Homeland Security, Internal Revenue Service, United States Postal Service, Department of Commerce, Securities and Exchange Commission, Naval Criminal Investigative Service, U.S. Army Criminal Investigation Commend, Federal Deposit Insurance Corporation, Commodity Futures Trading Commission, Federal Communications Commission, U.S. Department of Education and several non-profit organizations.

42 Project Safe Childhood National Public Awareness Campaign (http://www.projectsafechildhood.gov/)

43 *Electronic Media and Youth Violence: A CDC Issue Brief for Educators and Caregivers* (http://www.cdc.gov/ncipc/dvp/YVP/electronic_aggression.htm)

One of OnGuardOnline's most successful projects is the publication of *Net Cetera: Chatting With Kids About Being Online*,[44] a 54 page booklet that the agency provides free of charge. The Net Cetera project was mandated by the Broadband Data Improvement Act of 2008 which directed the FTC to "carry out a nationwide program to increase public awareness and provide education regarding strategies to promote the safe use of the Internet by children."

As of the end of May 2010, more than 3 million copies had been distributed through schools, police and sheriff's departments, and PTAs around the United States. The booklet deals with issues including social networking, cyberbullying, mobile phone safety, and protecting computers from malicious software. It's clearly written, based on facts and offers parents and other caregivers easy to understand messages to pass on to children and teens. The booklet emphasizes open lines of communication between parents and kids and advises parents to "be up front about your values and how they apply in an online context."

The Federal Communications Commission is also urging bold moves in the area of technology education. In his March 2010 speech outlining the "broadband plan for children and families," FCC chairman Julius Genachowski spoke of the "four pillars" of his plan: digital access, digital literacy, digital citizenship and digital safety. He called for "teaching kids to think analytically, critically and creatively" and pointed out that "digital citizenship means the values, ethics, and social norms that allow virtual communities, including social networks, to function smoothly. It means having norms of behavior that facilitate constructive interaction and promote trust." Included in the Chairman's definition of safety is, of course, freedom from cyberbullying and harassment but also helping kids deal with harmful websites such as those that promote eating disorders such as anorexia. The chairman highlighted distracted driving as a major concern regarding the safe use of technology.

In the National Education Technology Plan 2010 ("NET plan")[45] that it released in March 2010, the Department of Education called for significant educational reforms that could have a profound impact on Internet safety at school and at home. In what amounts to an endorsement of the use of Web 2.0 technology in schools, the department wants schools to include "the technology that professionals in various disciplines use," including "tools such as wikis, blogs, and digital content for the research, collaboration, and communication demanded in their jobs."

The document points out that "many students' lives today are filled with technology that gives them mobile access to information and resources 24/7, enables them to create multimedia content and share it with the world, and allows them to participate in online social networks where people from all over the world share ideas, collaborate, and learn new things. Outside school, students are free to pursue their passions in their own way and at their own pace. The opportunities are limitless, borderless, and instantaneous. The challenge for our education system is to leverage the learning sciences and modern technology to create engaging, relevant, and personalized learning experiences for all learners that mirror students' daily lives and the reality of their futures. In contrast to traditional classroom instruction, this requires that we put students at the center and empower them to take control of their own learning by providing flexibility on several dimensions."

In a section of the report entitled "Balancing Connectivity and Student Safety on the Internet," the plan addresses the question of whether filters, as required for schools that receive federal E-rate are helping or interfering. "Ensuring student safety on the Internet is a critical concern, but many filters designed

44 Net Cetera: Chatting With Kids About Being Online (http://www.onguardonline.gov/topics/net-cetera.aspx)

45 National Education Technology Plan 2010, US Department of Education (http://www.ed.gov/technology/netp-2010)

to protect students also block access to legitimate learning content and tools such as blogs, wikis, and social networks that have the potential to support student learning and engagement," it points out.

Neither this Working Group nor the Department of Education are necessarily opposed to the use of filters in school, but it is important to recognize that they may come at a "cost," if used in such a way as to block students from social media that could enhance their long-term online safety as well as education.

The NET plan recognizes the reality of how young people use social media and, rather than trying to suppress their use, incorporates those technologies into the learning environment, which can actually be protective. As we pointed out earlier, rather than increasing danger, it can be used to teach students to use these technologies, under the supervision of educators, in a safe and productive manner.

International efforts

While this Working Group is charged with focusing on efforts in the United States, it is important to put our work concerning a global medium into an international context. Just as the Internet makes possible innovative projects like the Flat Classroom Project, an international program that enables middle and high school students to reach across borders to work collaboratively with peers around the world, it also makes it possible for criminals from abroad to reach into American homes and schools. Whether it's the "Nigerian email scam," Trojan horse code written in Russia, or a foreign national trolling the Net to engage in sexual banter with American teenagers, the borders that separate our country from the rest of the world are extremely porous when it comes to the Internet.

Fortunately, there is some excellent work being done around the world ranging from the ground-breaking *Byron Review*[46] in the United Kingdom, which called for "a shared culture of responsibility with families, industry, government and others in the public," to work being done by the European Commission's Safer Internet Program. There is excellent work being done in New Zealand, Japan, Egypt and indeed every other corner of the world and it's important for U.S. educators, safety experts and policy makers to be in touch with their counterparts from other countries.

The Family Online Safety Institute's UK office is in the process of putting together an extensive international compendium of information about Internet safety which will be accessible at www.fosigrid.org when it becomes publically available. The aim of the Global Resource and Information Directory (GRID) is to bring together information, initiatives and best practices from every country into one easily accessible Web site.

RECOMMENDATIONS

The most important recommendation we can make is for all involved with Internet safety education to base their messages on accurate, up-to-date information. Of course, in a changing technology landscape, that's easier said than done, but we can do better.

KEEP UP WITH RESEARCH AND BASE EDUCATION ON IT

There needs to be a centralized clearinghouse at the federal level that disseminates the latest research to all concerned parties including federal, state and local agencies, school districts, professionals who

46 U.K. Byron Review: Children and New Technology (http://www.dcsf.gov.uk/byronreview/)

work with youth and the public at large. This clearinghouse should maintain a website with links to all relevant research material along with summaries written in easy to understand language. It should be updated as relevant research is published. This does not have to be a large or expensive operation as long as it is staffed by people who understand how to locate, summarize, and link to research from a variety of fields including social science, health, youth risk, risk prevention, social media, education technology, and law enforcement along with the latest technology advancements. In addition to summarizing relevant research as it becomes available, this office would also keep stakeholders up-to-date with technology advances that could have an impact on youth and youth safety.

COORDINATE FEDERAL GOVERNMENT EDUCATIONAL EFFORTS

While we are not calling for an "Internet safety czar," we are calling upon federal agencies and departments to coordinate their activities, both internally and with fellow agencies, to ensure that they are basing them on the same accurate research. There needs to be ongoing communications and interaction among all departments involved in Internet safety and education including Education, Justice, Homeland Security, Substance Abuse and Mental Health Services Administration (SAMHSA), Centers for Disease Control, Commerce, the FCC the FTC and the White House with liaisons to Congress and state and local agencies**.** Federal agencies along with, state and local authorities, members of law enforcement, industry and non-profit organizations need to work together as some have started to do with the FTC's OnGuardOnline. President Obama, in his Cyberspace Policy Review released on May 29, 2009, recommended that the United States initiate a K-12 cybersecurity education program for digital safety, ethics, and security and develop a public awareness campaign. As of this report's date of publication, intergovernmental coordination on these efforts was just getting underway.[47]

TARGET MESSAGING AND TREATMENT

It is very important that messages not only reflect actual risk (as identified in the research) but are also targeted appropriately. We need to focus prevention and intervention where they're needed. Having said that, we cannot ignore high-risk behavior on the part of a small minority, such as inappropriate in-person contact with an adult a minor has met online. That is why we are recommending that Internet education adopt the disease-prevention – and now risk-prevention – model of Primary, Secondary and Tertiary prevention and treatment for youth. Primary is prevention for all children, Secondary prevention targeted at specific risky behaviors and intervention at "teachable moments," and Tertiary prevention and intervention for youth with established patterns of risk behaviors.

PROMOTE DIGITAL CITIZENSHIP AS A NATIONAL PRIORITY

We need to recognize that, by far, the most common risk to children stems from their own actions and those of their peers and that many of these risks are not new. It is the delivery mechanisms which are. While technology can be used to amplify or facilitate bullying, for example, it is not the cause of the problem. In addition to sending a message that bullying and harassment will not be tolerated, work needs to be done starting in Kindergarten or earlier on "digital citizenship" – or rather a renewed effort to teach citizenship online and offline – encouraging children to respect themselves and others. This baseline (or "Primary") online-safety education cannot take place in a vacuum – or only in a single sphere of youth activity – but must promote movement toward greater civility not just among young people but also parents, educators, youth workers and other role models such as media personalities,

47 "Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure" (http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf)

public officials and candidates for office. The government can't legislate civility, but it can encourage it. This will not be an easy fix but, like cutting down on smoking, racism, sexism and other social ills, it can be accomplished through awareness-raising over time.

PROMOTE MEDIA LITERACY AND COMPUTER SECURITY AS A NATIONAL PRIORITY

Children should be taught media literacy, another Primary, baseline, online-safety skill, as soon as they first pick up digital media devices. Knowing how to understand words on a piece of paper, a web page or a TV broadcast is just the start. Children need to understand how to interpret what they read, see, and hear and learn to distinguish between fact, opinion and fiction. And in a social-media environment, media literacy has a new essential component: critical thinking about what is posted, shared, produced and uploaded as well as content that's consumed. Lessons on computer and device security can be taught in the context of learning the same critical thinking taught in media-literacy lessons. Students must be taught not only competency, privacy, and security in the use of technology tools but also the critical thinking skills that protect them from the social engineering behind false advertising and phishing scams.

While tools ranging from content filters to anti-malware programs have their place, they are not a substitute for the lifelong protection provided by critical thinking. The best "filter" is not the one that runs on a device but the "software" that runs in our heads.

CREATE A DIGITAL LITERACY CORPS FOR SCHOOLS AND COMMUNITIES

Consider FCC Chairman Julius Genachowski's proposal for a "Digital Literacy Corps" to "mobilize thousands of technically-trained youths and adults to train non-adopters." In addition to the Corps's community work, it could place trained, tech-savvy recent college graduates or university-age students into classrooms as digital-literacy and social-media experts who could provide an important first step in raising awareness of these critical topics for school-aged children and teachers alike. Programs such as AmeriCorps provide an interesting model for delivering much-needed services and information at the school and community level and coordinating funding for the volunteers who offer their service. Funding mechanisms such as reduced student loan obligations, stipends and other incentives for university age candidates to participate in this first wave of Internet Literacy and responsible Social Media use should be explored.

INCLUDE EVALUATION AS PART OF ALL FEDERALLY FUNDED ONLINE SAFETY EDUCATION PROJECTS

All federally funded online safety education projects should include an independent evaluation component to measure both what they teach and how effective the teaching has been. Evaluation should include changes in behavior as well as changes in knowledge and attitude.

ESTABLISH INDUSTRY BEST PRACTICES

Industry should be encouraged to maintain and expand best practices in consumer education, abuse reporting, customer service and tools/features for safety, privacy and security. Each company needs

to think through what it can do to protect and educate its customers and explore how it can best meet the needs of the different populations within its customer base, taking into account risk levels and other factors. When it comes to safety, the industry needs to work collaboratively with other companies, non-profits, schools and governments. While companies should not be encouraged to compete based on safety, they should recognize that maintaining a safe and healthy environment with respect for privacy is good for business.

Companies should make it easy for users to report abuse ranging from relatively minor terms of service violations to illegal activities and should have sufficient customer-support resources to quickly address these issues and, when necessary, pass them on to law enforcement or other appropriate agencies.

ENCOURAGE FULL, SAFE USE OF SOCIAL MEDIA IN SCHOOLS

Schools need to use and teach the same technologies students are using at home and between home and school. This means not only teaching the same use of social media on fixed and mobile technology, but using social media – in the form of wikis, video, podcasts, interactive word processing, online discussion, etc. – to teach regular subjects already taught in pre-K-12 classrooms. As a national educational priority, teachers of all subjects need professional development to help them understand how to use these technologies and to encourage their productive and safe use. Schools must also understand how to develop effective risk-management techniques and deploy policies, practices and initiatives that include their students' input.

AVOID SCARE TACTICS IN FAVOR OF THE NORMS APPROACH

While shocking stories can sometimes mobilize people, scare tactics simply do not work when it comes to long-term behavioral changes among youth. Scare tactics should be avoided in favor of educational campaigns that model positive behavior and marginalize improper behavior. This is not only true when it comes to harming others or being harmed by others, but self-harm as well. While this Working Group certainly agrees that it's a mistake for young people to allow themselves to be photographed in ways that might question their judgment, it is important to put even this into some perspective, given the number of youth who have engaged in such behavior relative to the ones who have suffered serious consequences. With all potentially negative behavior, it's important that adults do what they can to discourage it but avoid overreaction and "panic" when it isn't called for.

DEVELOP MORE EFFECTIVE RESOURCES FOR PARENTS

Parents need to be more actively engaged in stewarding young people's adoption of technology and safe practices. They need accurate information about risks, solid implementable ideas for the home, places to go to learn more, and clear information about what to do if a problem arises.

RESPECT YOUNG PEOPLE AND GET THEM INVOLVED

There is a commonly held belief that young people need to be protected from either criminals who are out to get them or from their own lack of judgment. While both can be true, it's also important to pay attention to research that shows that many young people have adopted and continue to adopt effective strategies to deflect dangers from both adult criminals and their misbehaving peers. This is

not to suggest that youth don't need adult supervision and support but prevention campaigns need to take into consideration the resources that young people bring to the table, both as participants and as leaders. Young people need to be involved in all aspects of risk prevention.

INTERNET SAFETY EDUCATION SUBCOMMITTEE: ADDENDUM A

ANNOTATED LIST OF INTERNET SAFETY EDUCATION LINKS

This list was developed and maintained by the California Technology Assistance Project[48], and any editorial comments contained in the list are those of the project and not the Online Safety & Technology Working Group.

Adina's Deck [Cyberbully Film Project]	Adina's Deck: Solving Cyberbully Mysteries. Three award-winning 30-minute films, website and parent/teachers guide to educate 9-15 year olds about Cyber Bullying, CyberPredators and Plagiarism. **School assembly details** are also available.	Education, Commercial
AT&T Education Advocates Program	AT&T Education Advocates/Directors are credentialed teachers who provide a variety of workshops to teachers, librarians, technology coordinators, and administrators. AT&T's Education advocate, **Linda Uhrenholt** has teamed with CTAP4 to help create and deliver our cybersafety materials.	Education, Commercial
AT&T Internet Safety Land	Developed by AT&T to teach elementary school children about safety and security while surfing the Web. Answer Internet safety questions to help the superhero capture the Internet villain. Complete all the tasks and kids earn a certificate of award. There is also a printable version of the game.	Commercial

48 The California Technology Assistance Project (CTAP) Region 4 (http://www.ctap4.net/projects/cybersafety/cybersafety-education-links-directory.html)

B4UCopy.org	The B4UCopy educational curriculum program has a goal of raising awareness of copyright laws and reinforcing responsible behavior online. Download the free curriculum for elementary and middle school students [**B4UCopy.org/kids**] or the high school curriculum [**B4UCopy.org/teens**] on copyright laws.	Nonprofit
B4USurf.org	Business Software Alliance (BSA) partnership site with an underlying theme of cyberethics and cybersafety. Includes cybersafety tips, teacher guides, cybersafety/ cyberethics lesson plans, free posters, an **interactive quiz**, and two **online games**. There's also a glossary about cybersafety and tips for parents.	Nonprofit
BeWebAware.ca	Funded by Bell and Microsoft, Be Web Aware is a national public education program on Internet safety with resources in both English and Spanish. Covers safety tips for all age groups, K-12 and a "Know the Risks" section on areas of cybersafety. There are links for reporting problems online. Affiliated with the **Media Awareness Network**.	Nonprofit
Berkman Center for Internet & Society	A research program at Harvard Law School founded to explore cyberspace, share in its study, and help pioneer its development.	Education
BNetSavvy.org	bNetS@vvy is a bimonthly e-newsletter offering parents and teachers tools to help kids, ages 9 -14, stay safer online. Primary focal areas include: social networking, wireless devices, gaming, cyberbullying and privacy. Two past issues were devoted to cyberbullying topics. The site is also translated into **Spanish**.	Nonprofit
Boston Public Schools Cyber Safety Campaign	The Boston Public Schools Internet Safety Website is a student-driven site that contains **downloadable resources** and strategies for **parents, teachers and students**. Check out their student video on **cyberbullying**.	Education
Braincells.net	Set in fictitious "Braincells High," Braincells covers computer and cellphone hacking, bullying, and cyberbullying. It teaches kids safe behavior and how to recognize unsafe behavior.	

BSA CyberTreeHouse	Business Software Alliance flash animation site. Includes videos, games, and other information for kids on how to keep cybersafe.	Commercial
BullyingNoWay.com	Learning environment created by Australia's educational community to address bullying, harassment and violence occur in all schools communities. Includes **anti-cyberbullying movies** created by students.	Education
ByteCrime.org	Industry-sponsored set of tools for keeping safe. Identify and protect yourself against threats like computer viruses, worms, spam, spyware, identity theft and online predators. Excellent **hardware security** and **wireless networking tips** can be found here. Their flash video tutorial on **phishing and spoof sites** is suitable for students. Download McGruff the Crime Dog's colorful kids' booklet, "**Mind What You Do Online**."	Nonprofit
Cafe Aspira	Organized by ASPIRA of NY, a Latino youth services organization. This site is dedicated to promoting cyber awareness, particularly within the Latino community, and to helping parents protect themselves and their children against cyber predators, bullies and frauds. Information on cyberbullying, cybersafety, cyberfraud and cyberpredators is available in English & **Spanish**.	Government
California Cybersafety.gov	The Department of Consumer Affairs has partnered with the California Coalition for Children's Internet Safety to help parents and community leaders protect our children in the online world.	
CTAP Region IV Cybersafety Project	Serves K-12 public education in California. Provides training materials, free posters and information for classroom teachers, school administrators, board members, law enforcement, safe school planning teams, parents and teens.	Education, Government
Center for Safe & Responsible Internet Use	Nancy Willard's site provides research and outreach for educators, parents, librarians and policy makers. Nancy is author of two books and has published extensively in professional journals. Check here for in-depth coverage of legal issues, presentation notes, reports and links to her publications.	Nonprofit

Chat Danger Online	Learn how to keep safe while chatting online. Practical advice for use of cell phones, chat, email, messenger and games. Includes real-life stories. Site developed by Childnet International.	Nonprofit
Childnet International	UK-based non-profit organization working with others to help make the Internet a great and safe place for children. Includes "Know It All" sections for teachers and parents. Connections are made to the ICT program of study. Many of the award-winning resources are available on a CD/DVD, free to local teachers. See also: **Digizen.org**	Nonprofit
ChildrenOnline.org	Workshops, research and tools for parents and schools with practical real-life solutions to the issues faced by young people online. Site was developed by two credentialed secondary teachers, who are also authors of a new ISTE book, **Safe Practices for Life Online**.	Education
Common Sense Media	Offers educator kits for **teaching digital citizenship**. See: **Internet Survival Guide** for Parents. Their video, "**A Common Sense Guide to Internet Safety**," would be ideal to present at a PTA Meeting.	Nonprofit
ConnectSafely.org	The ConnectSafely forum is co-directed by cybersafety experts, Larry Magid and Anne Collier. Forum, safety tips in English and Spanish, videos, printable tips.	Nonprofit
Crimes Against Children Research Center	University-based research center. Check here for the real stats, myths vs. realities on child predators. **Internet Safety For Teens: Getting it Right** is a fact sheet, packed with clarifying information for your next presentation.	Education
Cyber Exchange	Download free posters suitable for GR 6-12 classrooms on sexting awareness, firewalls, cyberpredators and cybersecurity from Cyber Exchange, a Cyber Security Awareness program and nonprofit that provides education and certification for information security professionals.	Nonprofit
Cyberbullyhelp.com	**Three school psychologists** (trained in Olweus Bullying Prevention techniques) have applied their knowledge and expertise to cyberbullying in the digital age.	Education

Cyberbully411.org	Cyberbully411 is an effort to provide resources for youth who have questions about or have been targeted by online harassment. The website was created by **Internet Solutions for Kids, Inc** with funding from the Community Technology Foundation of California.	Nonprofit
Cyberbullying Research Center	Two criminal justice specialists provide up-to-date information about the nature, extent, causes, and consequences of cyberbullying among adolescents.	Nonprofit
Cybercitizenship.org	The Cybercitizen Partnership was established by the Information Technology Association of America (ITAA) Foundation and the United States Department of Justice to establish a broad sense of responsibility and community in order to develop in young people smart, ethical and socially conscious behavior.	Nonprofit, Government
Cybercrime.gov	Department of Justice site on Cyberethics for Kids. Provides model acceptable use policies, info about being a good cybercitizen, rules for cyberspace, a **lesson plan outline** and links to other sites.	Government
Cybersavvy.org	A joint effort of the Direct Marketing Ass'n, AARP and **OnGuard Online** to help new and seasoned users protect their privacy and safely explore cyberspace.	Nonprofit
Cybersmart.org	Safety and skills for the 21st century. **Standards-based lesson plans** and activity sheets for K-12 students. The focus is on creative inquiry, fostering collaboration skills and critical thinking.	Education, Nonprofit
Cybersmart Detectives	From Childnet International and the Australian Government, this online game teaches four key internet safety messages and is designed to be played in a school environment. Limited to United Kingdom schools. A **promotional video** explains the project.	Nonprofit, Government
Cybersmart Kids Online	Community awareness project developed by the Australian Communications and Media Authority (ACMA). The site contains cyber rules, chat rules and mobile rules for kids as well as links to safe sites. Australian schools can also register for access to the online game, **Cybersmart Detectives**, in which players learn about managing bullying behaviors both offline and online.	Nonprofit

Digital Citizenship.net	KSU Professor, Mike Ribble's personal site on digital citizenship. The **Nine Elements of Digital Citizenship** should help shape educational efforts behind any cybersafety and cyberethics program.	Education
DigitalCitizenshipEd	Free online curriculum that focuses on creative rights in the world of digital citizenship. Addresses music, video, writing, software and images through thematic curriculum units that are ISTE aligned.	Nonprofit
Digizen.org	Practical advice on cyberbullying, using social networking sites safely and creatively, and being a good net citizen. Check out their **cyberbullying films** and teacher guides. Site is owned by Childnet International.	Nonprofit
Disney Online/Safe Surfing	**Safe Surfing with Doug**: 9 comic book style games and activities that help kids learn appropriate behaviors online (Disney UK Site).	Commercial
Dizzywood	Subscription-based virtual world with some free activities and content for kids. Click on the **video presentation** to learn how sixty GR 4-5 students in Marin County, CA used Dizzywood to learn about core social values and digital citizenship. More info about the school project is provided in this **podcast**, starting at 4:30 minutes into the broadcast.	Commercial
Don't Believe The Type	Missing & Exploited Kids site. Kids learn about the dangers of the internet, online chatrooms, instant messaging, social networking sites, situations to avoid and how to keep their identity private. Three **PSA's** are included. Resources are available in English and Spanish.	
EdZone/K12HSN	The California K-12 High Speed Network (K12HSN) provides this free suite of Web 2.0 tools to enhance today's classroom environment for students in the public school system.	Education, Government
Enough is Enough	Protecting our children online. Site focuses on public education about exposure to pornography and predators online.	Nonprofit

Family Online Safety Institute	International space for open discussion amongst stakeholders, exploring the challenge of how to keep children away from images, words and sites that their parents do not want them to see, and from behaving in ways that expose them to unnecessary dangers, without restricting wider online freedom.	Nonprofit
Family Resources Web Site [Symantec]	Symantec's Family Online Safety Guide won the 2008 iParenting Media Award and is a free download, available in English and Spanish. Register for the free newsletter. You can also find Internet Safety Advocate, **Marian Merritt's advice column** for parents here. Download articles from their **extensive library** or visit **Online Family Norton**, to learn about their product for managing kids' time online.	Commercial
FBI-SOS Internet Challenge	Internet safety program designed to help students recognize potential dangers associated with the internet, email, chat rooms and social networking sites. The program addresses and defines topics serious in nature such as seduction, child pornography, solicitation, exploitation, obscenity and online predators. Students participate in a **scavenger hunt**, take web-based quizzes and review specific web sites aimed at promoting online safety.	Government
GetNetWise.org	Developed by a coalition of Internet industry corporations and public interest organizations. This site provides a database of filtering tools for families: browsers for kids, tools that limit time on the computer, spam filtering tools etc. They have some helpful video tutorials on **using privacy settings with MySpace and Facebook.**	Nonprofit
Hector's World	Web-based animations and interactive educational activities in a rich graphic environment where elementary students learn digital citizenship skills. Take the **teacher site tour** or check out **teacher and parent** information. Each of the Hector's World episodes has accompanying **lesson plans** and storybooks. Part of **NetSafe**, New Zealand.	Nonprofit
Identity Theft Portal	Identity Theft Portal is an online resource for identity theft protection and identity theft victims. Provides information by State.	Nonprofit

IKeepSafe	Internet Safety Coalition with resources for parents and young kids, including **FunZone games**. Be sure to check out the flash tutorials on **Social Networking Basics** and their collection of **PSAs.** IKeepSafe provides digital citizenship training using a **C3 Matrix** of concepts: cybersafety, cyberethics and cybersecurity.	Nonprofit
iLearn Online	Partnership between iSafe and Microsoft to provide an "On Demand" system for Internet safety education. These training modules teach and/or train other educators on the iSAFE curriculum.	Nonprofit/ Commercial
Internet Safety with Professor Garfield	Online series of interactive, animated lessons. Comprised of a narrative tutorial (WATCH), guided practice (TRY), and an interactive challenge (APPLY), each lesson delivers a supportive and scaffolded learning environment for students. This site was developed in partnership with the Virginia Dept of Education.	Education
Internet Solutions for Kids (ISK)	Dr. Ybarra is an expert in the field of Internet victimization, with publications in cyberbullying, sexual solicitation, and related mental health and social characteristics of children. ISK has partnered with Dr. David Finkelhor and his colleagues at the **University of New Hampshire Crimes Against Children Research Center** to examine current issues in cyberbullying, blocking software, and more. ISK also hosts the site, **cyberbully411.org**.	Education
i-Safe, Inc.	i-SAFE offers a prevention-oriented Internet Safety Education program with interactive age-appropriate units of instruction designed for upper elementary, middle, and high school levels. There may be a fee for some materials.	Nonprofit
Join the C-Team	Comprehensive educational program of the Entertainment Software Association that introduces the concept of intellectual property to students in grades K-5 with hands-on activities that enable them to discover the natural connection between copyright and creativity.	Nonprofit

Kids Help Phone	Canadian nonprofit group offering phone and online counseling for kids. Be sure to check out their **PSAs** on bullying and cyberbullying.	Nonprofit
Kidsintheknow.ca	Kids in the Know is an interactive safety education program for increasing the personal safety of children and reducing their risk of sexual exploitation. Download a free copy of their colorful 16-page comic book [**Zoe & Molly Online**] for 4th grade students to address risks associated with children sharing personal information and sending pictures online. There is also a pre- and post-test.	
Kidz Privacy	Materials on this web site are provided by the FTC and are built around support for COPPA, the Children's Online Privacy Protection Act. Resources include basic advice for kids, tips for parents and downloadable teacher guides that include coverage of protecting student identities online.	Government
KinsaNet	The Kids International Safety Alliance (Kinsa) provides training for law enforcement and the general public on child exploitation. They work with well-known kids' properties to educate kids in environments that they know and love. Download their cyber safety comic, **Grossology: Web of Deception**. A **teacher's guide** is also available.	Government
KnowWhereTheyGo.org	Project Safe Childhood national media campaign to combat the increase of sexual predators using the Internet to entice and sexually exploit children. Stresses importance of knowing where your kids go online. Includes **video PSA's**, webisodes, radio PSA's and transcripts available in both English and Spanish. Site offers links to a **digital library** of free multimedia resources available by topic.	
Look Both Ways Foundation	Provides information on internet safety, security, privacy and ethics and a Skills for Life Online curriculum free of charge for K-12 schools.	Nonprofit
Make A Difference for Kids, Inc.	Non-profit organization dedicated to the awareness and prevention of cyberbullying and suicide through education.	Nonprofit

McGruff.org	Internet Safety stories, games, videos and tools for kids and parents from McGruff and the National Crime Prevention Council. Download their poster, **Internet Rules of the Road**.	Nonprofit
Media Awareness Network	The Media Awareness Network has created games and interactive student modules for K-12 students (complete with extensive Teacher's Guides) to help kids to develop cybersafety skills. Site is also accessible in **French.**	Education
Megan Pledge	Named in honor of Megan Meier, who took her own life rather than face continued harassment at the hands of a neighborhood mom posing as a cute 16-year-old boy. The campaign seeks one million teens to take a pledge against cyberbullying in Megan Meier's name.	Nonprofit
Michigan Cyber Safety Initiative (CSI)	Includes templates and handouts for student, teacher and community workshops as well as **videos** from other agencies.	
MindOh!	Download their "Cyberbullying Thinking it Through" worksheets and use them as discussion starters with kids. Students assess their own beliefs and attitudes, consider past experiences, and explore ways of making smarter choices in the future. Cyberbullying Lesson Plans are also available on cyberbullying, predator and privacy topics.	
MySpace Dept. of Safety & Security	Safety videos, MySpace Guides for Parents and School Administrators, **ParentCare Software** downloads, and flash tutorials on **social networking basics**.	Commercial
MySpace MyKids	Interactive video sessions that educate parents on MySpace and equip them to tackle the online issues that teens may face.	
MySpace Pause	A collaboration between Fox Network Group and Kaiser Family Foundation. Stay informed and stay in control. It only takes a minute to change your life. That's one minute to stop, think, pause and consider the consequences of your actions. Site includes PSAs and informational resources.	Commercial Nonprofit

NetAlert Cybersafe Schools	NetAlert is the Australian Government's online safety program. Primary grade students can follow a flash animation adventure called **CyberQuoll** while students in secondary grades have their own hip adventure called **Cybernetrix**. Teacher support materials are also available.	Government
NetBasics.org.NZ	Launched in April 2008, this award-winning site from New Zealand is composed of 10 highly entertaining flash animations following the travails of the Jones family as they negotiate their way around the Internet. The series includes a collection of good and bad characters in fictional adventures that engage users while they deliver a serious message about the security threats we face every day online.	Government
NetFamilyNews	A weekly electronic news service to inform and educate parents, families and caregivers of children who spend time online. Well written, accurate and timely information from Internet Safety expert, Anne Collier.	Nonprofit
NetSafe, NZ	NetSafe provides cybersafety education for all New Zealanders - children, parents, schools, community organisations and businesses. The ISG has been designated the Ministry of Education's 'agent of choice' for cybersafety education in New Zealand.	Nonprofit
Netsmartz.org	Interactive, educational safety resource from the National Center for Missing & Exploited Children® and Boys & Girls Clubs of America for children, aged 5-17, parents, guardians, educators, and law enforcement. Great **"real life stories"/flash videos** and **activity cards** for classroom use and lots of online/ offline activities for younger kids. Activity cards are also available in Spanish.	Nonprofit
Netsmartz Education	Instructional and classroom materials and videos in both English and Spanish, coded for grade-level appropriateness. Train-the-trainer materials are also available. A drop-down menu provides direct links to pages customized for each state, to make it easy to form educational partnerships.	Nonprofit
Netsmartz 411	Internet Safety Help Desk	

Nortel IT	An initiative of Nortel Community Relations to prepare teachers, students, and learners of all ages to develop 21st century skills. Lesson plans, guides, activities, PowerPoint files and videos cover digital citizenship topics like **viruses and spam**, **digital ethics**, **predation** and **cyberbullying**. The site is translated into multiple languages, including **Spanish**.	Commercial
Northwest Learning Grid(NWLG)	Educational site from England uses colorful graphics and flash-based quizzes to test student skills in **digital literacy**. Most questions focus on conducting useful searches and finding the best information. Elementary and secondary students can also play five **e-Safety games** to demonstrate knowledge of appropriate online safety behaviors.	Education
NSTeens.org	Part of Sprint's 4NetSafety Program. Content for this site was created by NetSmartz and covers topics like social networking and cyberbullying. The site uses flash-based **comics** and **videos** to explain how to use the Internet safely and avoid cyber-bullies and predators.	Nonprofit
OnGuardOnline	FTC site that provides practical tips from the federal government and the technology industry on topics such as identity theft, spyware. phishing, spam and ecommerce/ shopping online. Their colorful flash-based quiz section would be great for student use and includes **13 games** that help kids test their cybersmarts. Resources are available in English and **Spanish**. Schools can order bulk copies of **NetCetera: Chatting With Kids About Being Online** to send home to parents.	Government
OnlineFamily.Norton	Parental control service that allows parents to manage and monitor their child's time online. Watch this **video** to see how it works. There is a subscription fee involved.	Commercial
Passwords are like underwear... Poster Program	Developed by the IT Dept at University of Michigan, this series of five clever posters gets users to remember and adopt a few basic principles of password security. You can order copies off of their web site.	Education

PBSkids.org: Get Your Web License	If kids answer all 10 questions about surfing the Internet correctly, they may print themselves a web license.	Nonprofit
Play It Cybersafe	Learn about cybercrimes. The Cyber-Crime and Intellectual Property Theft Prevention and Education Project is a United States Department of Justice funded initiative to educate the public on cyber-crime and intellectual property theft.	Government
PointSmartClickSafe.org	The Cable Industry's effort to educate parents about protecting their child's identity online. Click on the video link at the bottom of the page to access six flash videos: Internet Safety Pledge, media literacy, phishing and predators, kids' blogging content, privacy issues, etc. Resources are in English and Spanish.	Commercial
PowerToLearn.com	Interactive case studies exploring 8 topics: Wireless, Social Networking, Digital Permanence, Cyberbullying, Misinformation, Fair Use, Privacy and Downloading. Through multimedia activities, students examine issues affecting school work, class papers, entertainment activities, and online safety. "Power to Learn" is Cablevision's nationally-recognized education initiative. Some resources are available in Spanish.	Commercial
Professor Garfield Foundation: Internet Safety & You	Garfield animated comics educate kids about cyberbullying, online safety. Other topics in development include digital and media literacy. Students watch animated lessons, try interactive, guided practice and apply knowledge to earn safety certificates. Includes downloadable teacher lesson plans. A joint project of the Virginia Dept. of Education and the Professor Garfield Foundation.	Government/ Nonprofit
ProtectKids.com	Practical advice on internet dangers, including pornography and sexual predators from Donna Rice Hughes, author of **Kids Online: Protecting Your Children in Cyberspace.**	
Rochester Regional Cybersafety & Ethics Initiative (RRCSEI.org)	Rochester Institute of Technology-led community effort to improve cyber safety, security and ethics at the K-12 level. Educator partnership with NetSmartz. See also their findings from a 2007-2008 **RIT Survey of Internet and At-Risk Behaviors of 40,000 K-12 students [PDF].**	Education

SafeKids.com **SafeTeens.com**	Safe Kids.com and SafeTeens.com are blogging sites operated by cybersafety expert, **Larry Magid** and in connection with **ConnectSafely.org**. The sites contain information about the dangers of children using the Internet, rules, advice, and tips relating to child security and the web.	Editorial
SafePassageMedia	Bullying prevention program and **award-winning videos**. SafePassage Media was formed in 2007 for the sole purpose of creating and distributing two public awareness DVDs related to the suicide of 13 year old Ryan Halligan, a cyberbullying victim.	Nonprofit
SafeSurf Kids	Florida's Internet Safety site for young kids. Kids can learn about the Internet with games and activities. See also, the SafeSurf companion site for **teens**.	Government
Simple K12 InfoSource	In addition to the online curriculum and training lessons, the program includes assessments, quizzes, and a safety pledge for students, safety plans for teachers, and a self-assessment and resources for parents.	Commercial
Smart AUP	The Smart AUP is a fast, simple, assessment tool designed to allow students to demonstrate their knowledge of the rules and provisions outlined in a standard Acceptable Use Policy (AUP). Developed by **FBI-SOS** for the State of Florida.	Education, Government
Smart Online/Safe Online (SOSO)	Non-profit social initiative that uses kids to deliver campaigns aimed at educating their peers about cyberbullying/cybersafety issues. Check out their **video** on cyberbullying and an online game called "**Web Warriors**" where kids create their own avatars and complete missions that educate them about cyberbullying, social media and mobile safety.	Nonprofit
SocialSafety.org	Started in January 2008 by the founders of MyYearbok.com, SocialSafety.org is an effort to educate U.S. teens on the dangers of social networking. Social Safety provides hundreds of thousands of free safety education packets for U.S. high school students, and provides free safety content to any student or site that requests it.	Nonprofit

StaySafeOnline.org	The National Cyber Security Alliance (NCSA) is a collaborative effort among experts in the security, non-profit, academic and government fields to teach consumers, small businesses and members of the education community about Internet security.	Nonprofit
StopBullyingNow!	U.S. Department of Health and Human Services offers flash movies, games, and information about bullying and how to prevent it. Some of the flash movie "**webisodes**" focus on cyberbullying. Closed captioning and Spanish versions are available.	Government
StopCyberbulling.org	Part of the Wired Safety group's effort. Includes a flash presentation, Parent's Guide to Cyberbullying.	Nonprofit
SurfSwell Island	Adventures in Internet Safety with Mickey and the Gang, delivered in typical Disney style. Features include "smart-surfing" lessons where kids learn about privacy and netiquette through entertaining and interactive activities, educational games, and hands-on experiences.	Commercial
That's Not Cool	Web site developed by the National Teen Dating Abuse Hotline. Great **PSA's** on teen abuse of technology through controlling behaviors like excessive text messaging, pressure for digital photos, stalking, privacy problems and rumors.	Nonprofit
Trend Micro Web Security and Internet Safety	Commercial company with an interest in promoting Internet Safety for kids. Content covers privacy issues, mobile safety, identity theft, cyberbullying and computer security issues. There is also an **Internet Safety Blog** for Parents and Schools.	Commercial
The Children's Partnership	National nonprofit, nonpartisan child advocacy organization - goal is to ensure that **digital opportunities are available to all young people**, especially those that are low-income and underserved. **ContentBank** is one of their affiliated web sites. Great video here, "**Why Does Technology Matter for Youth?**" Agency also has downloadable PPTs and guides for child safety online.	Nonprofit

The Socrates Institute/ CyberEthics Project	An educational program to address the problem of juvenile cybercrime. The K-12 project in CyberEthics is in development and will have classroom, video, and web-based learning materials including videos of actual case studies of juvenile cybercrimes (e.g. hacking, software piracy, illegal downloading, cyberbullying).	Education
Virtual Global Task Force	The Virtual Global Taskforce (VGT) is made up of police forces from around the world working together to fight online child abuse. Check out their PSA, "**Think You Know Who You are Talking To?**"	Government
Web Wise Kids	Community and parental resources for Internet safety. They have developed three interactive cybersafety adventure games (**Missing**, **Mirror Image** and **AirDogs**) that are excellent for classroom use. WWK was recently awarded funding from Verizon to develop a game to educate students about responsible use of cell phones. **Katie Canton's story** (told on video) is also excellent for student learning.	Nonprofit

INTERNET SAFETY EDUCATION SUBCOMMITTEE: ADDENDUM B

EXAMPLES OF INDUSTRY-PROVIDED NET SAFETY PROGRAMS

AOL

AOL has been a strong advocate of Internet safety since its early days as the nation's largest dial-up online service, when it pioneered the use of parental controls, special kids-only services, and Internet safety information. In 1996, AOL became the sponsor of one of the nation's first Internet safety websites and, despite a rather tumultuous existence since its merger with Time-Warner in 2000 and subsequent separation in 2009, AOL has remained committed to Internet safety.

The company operates a SafetyClicks blog (blog.safetyclicks.com/) featuring industry and advocacy experts who provide parents, teens and kids with information and tools to help keep themselves and their families safer online. The blog covers a wide variety of topics related to child Internet safety, social networking, cyberbullying, sexting, sharing information online, Internet lingo, and more. AOL also operates AOL Internet Security Center where it has educational materials and tools for computer security.

A company official said that AOL works within the educational community to bring Internet safety to the schools by providing online safety education in the form of formal presentations or hands on demonstrations at schools, for PTA meetings, and other organized meetings. AOL also supported the Virginia Internet Safety Curricula requiring state schools to provide an online safety course and, internationally, AOL worked with teachers and education authorities to develop Internet safety materials and lesson plans specifically for teachers. AOL provides context-specific safety messages in areas where young people and others make decisions about how to interact with the community.

The company provides support to nearly a dozen national-level Internet safety organizations offering a variety of programs and materials to schools and families.

AT&T

AT&T's "Stay Connected, Stay Safe site" (att.com/safety) offers safety tips and interactive safety games for both its wireline and wireless services. Its "Wireless Smart" section, for example, includes "a parents' guide to texting" and information about its "Smart Limits" program that enables parents to put controls on their children's phones. There is also extensive Internet safety information including access to PDF files of some of the company's printed brochures for distribution offline.

AT&T has taken the initiative to combat the dangerous practice of texting while driving with a campaign called "It Can Wait." The new national campaign, according to a company press release, "features true stories and the text message that was sent or received before someone's life was altered, or even ended, because of texting and driving." FCC Chairman Julius Genachowski mentioned distracted driving in his "broadband for kids" speech: "A quarter of U.S. teens with cell phones say they have texted while driving," he said, adding that "according to the National Highway Transportation Safety Board, 80% of fatal teen accidents are caused by distracted driving."

The company also took its safety show on the road through the AT&T Hometown Tour, which, according to AT&T "visited more than 100 communities nationwide and worked with more than 20,000 students from Connecticut to California on Internet safety lessons, programs, and workshops geared toward elementary and middle-school-aged students." AT&T also supports the consumer-safety education programs of a number of national Net-safety advocacy organizations.

Comcast

In October 2009, Comcast unveiled its Constant Guard Internet Security Program, designed to protect its broadband customers from bots, viruses, and other online threats. The program provides protection to children, whose email accounts can be spammed by bots with links to objectionable content.

As a part of its partnership with Symantec, Comcast HSI customers have access to OnlineFamily.Norton at no additional charge. OnlineFamily.Norton gives parents the ability to monitor where children go, how long they are online, who they talk to, and what information they are sharing with others.

Comcast and Kidzui have a partnership to deliver a safe, fun Internet portal for kids and families to millions of households across the country. Designed for children aged 3-12, KidZui connects kids to games, activities, videos, and educational materials – all of which has been reviewed by an editorial team of parents and teachers.

As part of National Internet Safety Month in June 2009, Comcast and McAfee partnered to call on parents and their children to take the *Cyber Summer Safety Challenge*, designed to start a dialogue about Internet safety and online threats, and what children and teens can do to protect themselves.

The Challenge included both a kid's version and a teen version of online safety issues for parents and their children to talk through. Comcast also works with Internet safety organizations such as FOSI and iKeepSafe.

In its partnership with iKeepSafe, Comcast rolled out state-specific Internet safety "Parent Presentations" in several states, including Florida, Maryland, Michigan, Mississippi, New Hampshire, Texas, Virginia, and Washington, in 2008 and 2009, in coordination with each state's Attorney General. Comcast has coordinated efforts to distribute these Parent Presentations throughout the schools in these states and continues to host these Presentations On Demand for its video customers. Comcast has also sponsored and helped distribute Faux Paw and the Dangerous Download in the Faux Paw series, a book and DVD series that educates children about the dangers and potential pitfalls online.

Comcast provides Comcast SafeSearch, a kid-safe Internet search tool, powered by Google. Comcast also offers an email feature that enables parents to limit who their children may receive email from (e.g., parents can create a specific list of individuals who are allowed to send email to their children, thus blocking email from spammers advertising material parents may find objectionable).

Finally, Comcast implemented controls that allow authenticated customers using the new Fancast Xfinity TV service to set up account "families" consisting of primary and secondary account holders. Primary account holders can restrict secondary account holders' access to Fancast Xfinity TV content, either by network or by rating. Users within a particular family account have to enter a four-digit PIN prior to viewing a video that has been restricted on that account. In connection with these controls, Comcast uses an opt-in feature contemplated by the Children's Online Privacy Protection Act (COPPA), which prompts a primary account holder, during the online parental control set-up, to read and complete a COPPA disclosure and a COPPA consent screen. For each restricted secondary account, a primary account holder must affirmatively consent to the collection and use of personal information for children under 13 years of age.

Facebook

Facebook has a privacy link at the bottom of each page and, as of this writing, was in the process of building out a Safety Center with help from its Safety Advisory Board. The growing safety board currently consists of representatives of six national and international non-profit organizations. Facebook also provides funding to support these organizations' own consumer-education programs.

In December 2009, Facebook announced new privacy settings and took the unprecedented step of requiring all of its members to configure their privacy settings. Although there was some pushback about the company's default settings, the exercise forced more than 300 million people around the world to put at least some thought into privacy.

In addition to its safety education pages, the company builds "contextual messaging" into the product. For example, when news users go through the registration process they are introduced to some basic concepts, but as they start posting information on the service they are reminded about privacy options. For example, when someone updates his status, there is a little lock icon that shows the current privacy settings for that piece of content and allows the user to change those settings.

As part of a court settlement, Facebook has agreed to allocate $6 million to an independent foundation that will fund research- and advocacy-related programs in the areas of user privacy and safety. In addition to the non-profits it supports, Facebook also supports the national Crimes Against

Children Conference presented annually by the Dallas Children's Advocacy Center and the Dallas Police Department.

Microsoft

Microsoft focuses on three areas to make computing and the Internet safer for children. These three areas are 1) tools and technology, 2) guidance and education and 3) law enforcement and public policy.

Microsoft builds free family and safety tools and parental controls into a range of products and services, including Windows operating system; Windows Live online services; the Xbox 360gaming platform and Xbox LIVE online gaming environment; the Zune digital media player; and the Mediaroom digital video platform. These tools let parents decide when children can use the computer, which Web sites they can visit, which software applications they can use, which games they can play and with whom they can interact online. In addition, Microsoft provides Windows users a free anti-virus and anti-malware program.

Microsoft's online safety and privacy center (www.microsoft.com/protect) provides safety, privacy and security guidance. This site includes brochures and videos covering topics from safer online gaming and social networking to building stronger passwords and avoiding cyberbullying.

In 2009, Microsoft launched a public service initiative called Get Game Smart (www.getgamesmart.com) with more than a dozen children's media advocacy groups. The Get Game Smart campaign is dedicated to educating families about safer and more balanced digital media consumption.

Microsoft partners with government agencies and NGOs to encourage comprehensive public education on safer, more responsible behavior online. In addition, Microsoft helped develop the Federal Trade Commission's online safety Web site, OnGuardOnline.gov.

MySpace

MySpace has a "Safety tips" link at the bottom of every page which includes links to safety videos, tips and settings, and resources from a variety of national and international non-profit groups. The company, according to officials, offers educational materials targeted to different constituents, including law enforcement, schools and parents. Resources include a guide called *MySpace Safety for Parents and Educators*. MySpace and News Corporation Chief Security Officer Hemanshu Nigam (who is co-chair of this Working Group) has his own MySpace page, where he blogs about online safety and security, especially as it applies to MySpace. He also speaks frequently at law-enforcement conferences.

The company created a guide specifically for law enforcement and has trained more than 4,000 police officers in person. A guide has been distributed to more than 100,000 school officials. MySpace provides dedicated toll-free numbers to connect law enforcement and school personnel to its customer-service department when user behavior becomes harmful.

MySpace is currently or has previously partnered with a number of non-profit agencies, organizations, and associations and works with the Internet Crimes Against Children Task Forces (ICAC) nationwide.

In its site, MySpace offers contextual training in addition to the centralized safety learning tools it provides. For example, as a user clicks on a link that takes him off the site, he is warned that he's going

to a page not vetted by MySpace. There are even more strenuous warnings if a user is about to go to a page believed to contain malicious software, according to a company official.

Ning

Ning is a unique, rapidly growing social network service that currently hosts some 2.3 million user-created, interest-based or "vertical" social network sites that together serve about 45 million people. Ning gives moderators, the people who set up their own networks, control over who can access them and how they're used and policed.

Ning has a safety center that provides general safety tips and a set of tips aimed at teens and another for parents. There is also instruction to help members use the services privacy and safety controls. Ning also engages its members to provide input on what is and isn't working when it comes to safety and privacy tools.

The service has a robust Help Center that offers tutorials to help moderators set up and manage their sites' privacy and safety tools. Because the network moderator or community leader has so much control, the service has been attractive to teachers, many of whom have set up networks for the exclusive use of their students or perhaps their students and parents. Teachers who are using Ning (or other services) in the classroom afford students opportunities to learn safety, privacy and citizenship in the context of the subjects being taught with Ning.

Ning provides support for several Net-safety nonprofit organizations and works closely with the National Center for Missing & Exploited Children, according to a company official. The company also participates in a Cyber Hate Strategy Group organized by the Stanford Center for Internet and Society and the Anti-Defamation League. This group consists of members in industry, academia and NGO's and will examine approaches of tackling the problem of cyber hate.

Verizon

Verizon's Parental Control Center (http://parentalcontrolcenter.com/) not only provides access to how-to information about the company's parental control tools but also to advice about mobile and online safety. This includes links to resources from NetSmartz and other programs educating youth and parents on a variety of safety topics. The Verizon Foundation's ThinkFinity.org site provides materials for teachers and parents on identity protection, Internet and mobile safety and related topics. Verizon and its foundation provide support for a variety of safety projects including conferences and the recently aired PBS Frontline program *Digital Nation*.

Yahoo

Yahoo operates a safety site (safety.yahoo.com) that has separate areas for teens and parents. The teen section has resources and links to teen-centered safety programs including iMENTORs and WiredSafety's TeenAngels. The parents section and the main page have links to Internet safety bloggers from a number of national Internet-safety organizations. The site also hosts comprehensive guides for safer practices in using its mail, online groups and mobile service. There is also safety information in the parents sections of Yahoo Kids and Yahoo Shine, with links to safety articles written by Yahoo staff and safety experts from non-profit organizations. There are also sections with "tools and tips" that deal with a variety of safety-related subjects

The company works with law enforcement to educate middle school students on safer practices by offering annual assemblies and has helped law enforcement create an original "restorative justice" diversion course for youth who have mistakenly engaged in risky online behaviors.

Yahoo also organizes and hosts an annual CyberCitizenship Summit for educators and child safety experts to discuss methods for helping students use technology in positive ways, manage their digital reputations, and help prevent abuse such as cyberbullying.

The company supports the educational work of a number of non-profit Internet safety organizations and associations.

YouTube

Google's YouTube isn't a social network site in the traditional sense, but it is very much a social-media experience as a place online where people establish profiles, channels and playlists, express themselves via video and use both video and text to comment on one another's videos. YouTube uses its own medium (as well as text) to educate users about safety through animated video tutorials.

There is a link to YouTube's safety section at the bottom of its home page. As soon as you land on that page you see and hear a short (1:46) video providing basic guidelines to protect one's safety and privacy with messages that include "don't put up with bullies" and "don't be a bully." The video also advises kids, "If something happens that makes you uncomfortable, tell a trusted adult."

YouTube has additional videos and articles on a variety of safety and privacy subjects including cyber citizenship, privacy, teen safety, hateful content, sexual abuse of minors, harassment and cyberbullying, suicide, impersonation, spam and phishing, and harmful and dangerous conduct.

The company recently instituted a "Safety Mode" tool to give parents and others the ability to filter out potentially objectionable content. Users can turn Safety Mode on or off by clicking on a link at the bottom of any page, and it can be locked into position until the user logs in and enters a password.

YouTube's parent company, Google, provides financial support to a number of Internet safety projects.

SUBCOMMITTEE ON PARENTAL CONTROLS & CHILD PROTECTION TECHNOLOGY

PURPOSE & SCOPE OF SUBCOMMITTEE

According to our authorizing statute, part of OSTWG's congressional mandate was: "*To review and evaluate… the status of industry efforts to promote online safety through… parental control technology, blocking and filtering software, age-appropriate labels for content or other technologies…*" and to study "*the development of technologies to help parents shield their children from inappropriate material on the Internet*."

The working group's investigation in this and other areas was constrained to some extent by the Paperwork Reduction Act of 1990. Department of Commerce officials notified OSTWG members that we would not be able to solicit input from outside third parties. Consequently, the scope of the review conducted by OSTWG members was limited to those we were able to hear from, what we were able to gather on our own, and our own personal knowledge of these issues and experience in this field.

We were, however, able to personally hear from several leading experts in the field during our meetings together. Among those who presented before the task force on these issues:

- AOL – **Karen Hullenbaugh**, Director of Safety Products
- Common Sense Media – **Todd Haiken**, Senior Manager of Policy
- CTIA–The Wireless Association – **Dane Snowden**, Vice President, External and State Affairs
- Digimarc – **Stuart Rosove**, Vice President for Media & Entertainment
- Entertainment Software Rating Board – **Patricia Vance**, President
- Facebook – **Chris Kelly**, formerly Chief Privacy Officer and Head of Global Policy
- Federal Communications Commission - **Kim Mathews**, Attorney Advisor, Media Bureau, Policy Division
- Federal Trade Commission – **Phyllis Marcus**, Senior Staff Attorney, Division of Advertising Practices
- Internet Safety.com / Safe Eyes - **Forrest Collier**, Chairman & CEO
- Google - **Scott Rubin**, Global Communications & Public Affairs
- Loopt – **Brian Knapp**, Chief Operating Officer
- Microsoft – **Frank Torres**, Director of Consumer Affairs
- Motion Picture Association of America – **Orit Michiel**, Vice President and Domestic Counsel
- MySpace – **Hemanshu Nigam**, Chief of Security
- National Cable & Telecommunications Association – **Rob Stoddard**, Senior VP, Communications & Public Affairs
- Ning – **Jill Nissen**, Vice President, Chief Policy Officer

- RuleSpace – **James Dirksen**, Managing Member
- Symantec – **Marian Merritt**, Internet Safety Advocate
- Think Atomic – **Cheryl Preston**, Brigham Young University Law School
- USTelecom – **Kevin Rupy**, Director of Policy Development
- Walt Disney Company / Club Penguin – **Susan Fox**, VP, Government Relations
- Yahoo! – **Emily Hancock**, Senior Legal Director
- Zynga - **Reggie Davis**, General Counsel

These experts and members of the task force were asked to comment on a variety of questions that the task force was pondering, including:

1. Generally speaking, how well do you think the parental controls **marketplace** (broadly-defined) is functioning? What works particularly well? Conversely, what isn't working so well?
2. How do you measure **effectiveness** in this context?
3. What could be done to generate greater **awareness** or uptake of parental controls or child protection technologies?
4. How do you feel about **default settings**? Should media and technology providers establish more restrictive defaults for their products and services? Should the government mandate or "nudge" providers to set defaults more restrictively?
5. What is the proper **role for government** in this context?
6. What sort of **additional studies and research** would be useful going forward? What questions deserve more study?

After providing a brief sketch of the current market of parental control technologies, a summary of our thoughts and findings about these six questions will follow. Further elaboration and input from various task force members and expressions of minority views can be found in an appendix to the report.

A BRIEF SKETCH OF THE CONTOURS OF THE PARENTAL CONTROLS MARKETPLACE

The parental controls marketplace continues to evolve rapidly in response to changing market realities and needs.[49] A diverse array of parental control technologies exists, and they can generally be grouped as follows:

- **Independent / "Client-Side" Filters and Monitoring Tools**: Until recently, most filtering software was purchased at retail stores or downloaded from websites, and installed on the user's personal computer. These stand-alone or "boxed" filtering solutions are often referred to as "client-side" filters (because in technical terms a web browser is commonly called a "client" that can access content on a web "server"). These client-side

49 A comprehensive and constantly updated list of filter providers and other parental control tools can be found on David Burt's "GetParentalControls.org" blog: http://getparentalcontrols.org/product-guide. Sites such as GetNetWise (http://www.getnetwise.org) provide parents with information and links to filtering programs and educational tools.

solutions are still very popular and many different vendors continue to compete in this market (although some vendors develop for the commercial market while others focus on the consumer market). The market for parental control products is quite deep and constantly evolving with the addition of new tools with a variety of features. These software tools let parents block access to adult content and other problematic websites and typically let parents impose time constraints on their children's computer and Internet usage. Some offer filters that screen certain inappropriate or problematic content based upon the parents' selections or the age of the child. Some only allow access to pre-approved sites, to avoid a problem site getting through the filter. These are called "white lists" or "green lists." Such preapproved lists present a challenge in that new (and unreviewed) content can easily be added to a website. Some tools use technology to screen content on the fly based on keywords and algorithms to block adult and other problem content. These catalogues of prescreened inappropriate sites are called "black lists" or "red lists." Other tools combine the two types of list, and there are challenges for both approaches. While early on human screeners may have been able to handle content review, the exponential increase in user-generated content has made this approach much more challenging and often costly.

Increasingly, standalone products and software packages offer robust monitoring tools that give parents several options, from being able to see each website their children visit, to viewing every e-mail or instant message that they send and receive, to recording their keystrokes, including every word that they type into their word processors or chat conversations, or showing every activity online or on the computer offline. While some products only produce a report accessible on the computer they are monitoring, many of these monitoring tools can even send parents a periodic report by email or text message summarizing their child's Internet usage and communications. More robust software programs even allow parents to capture screen shots of sites their kids have visited, images they send or receive, and other activities.

Some of these products operate for select accounts only – and can be set for children on a child-by-child basis, while others operate for all computer users. Some of these products offer an optional "stealth mode." In stealth mode, once the software is installed on the computer, it is largely invisible to the monitored user and all other users. In open mode, on the other hand, notices may appear when the computer is turned on or the monitored user logs into their account (which can thereby promote dialog between a parent and child about appropriate Internet content). Another option is a tool that permits parents to identify the images that have been accessed on a computer even if the search history has been erased. Some parents find that a child's awareness of this capacity provides incentives for safer online practices.

Filtering is typically obvious to users, as most programs display a message that the site is unavailable due to the filtering or blocking features of the program. Some filtering products, however, merely block the site and the child receives no explanation about why the site cannot be viewed. The child may believe that the site is down, the computer or Internet access is malfunctioning or, should the child be aware of the filter, that it may be blocked. Newer products allow the child to notify their parent or caregiver that they have been denied access to a site and ask their parent to override the filter to allow the site to be viewed, or to change their access permissions from the parent dashboard accessed online from wherever the parent has Internet access.

- **ISP-Integrated Parental Controls and Filtering Tools**: The stand-alone or "client-side" filtering solutions, such as those described above, dominated the online parental controls marketplace in the late 1990s. But the market has changed significantly since then. Today, many Internet service providers (ISPs) and online service providers offer parental control services. These options are usually offered (but not usually provided as a default), to subscribers as part of an integrated suite of security tools, which typically include anti-virus, anti-spyware, and anti-spam tools. These security options are often offered free of charge, or for a small additional fee, when subscribers sign up for Internet service. Some are offered free to all Internet users. Most of these integrated tools offer automatic updates so consumers don't have to manually download upgrades to stay current. Thus, millions of parents now have free or inexpensive Internet parental control tools at their disposal, either through their Internet service provider or other online provider. Of course, parents can also add on other tools or independent filtering and monitoring solutions such as those outlined above.

- **Digital Footprint Searches**: Some services help parents keep track of their children's "digital footprints" by allowing them to search for and view publicly available content posted by and about their children online. These types of tools attempt to collect material from across the web, including public profile information from social networking sites, photo-hosting sites, and blogs or message boards, making it easier for parents to keep tabs on their children's online activity. The reports these services generate can serve as the starting point for important conversations between parents and children about what type of material is appropriate to share publicly, and can help children, teens, and adults get a better sense of what counts as "public" in the online space. Because some online information is not public, these services only provide a partial picture of online information.

- **Operating System Controls and Web Browsers Controls**: Companies such as Microsoft and Apple have integrated some parental control features into their computers' operating systems. The web browsers that these companies offer (Internet Explorer and Safari) work in conjunction with the OS-level controls or other parental control software. Parental control add-ons are also available for the Mozilla Foundation's Firefox browser. Some parental control providers offer a "kid browser" that will give a child their own kid-friendly browser that restricts access to all sites and services aside from those pre-screened and approved for children. These limited kid browsers are much less useful for older children who use computers for research and social interaction.

- **"Safe Search" Engine Filters**: Many major search engines and video-sharing service providers (such as YouTube) offer "safe search" filters that filter objectionable content from search results. This can help block a great deal of content that children might inadvertently stumble upon or intentionally seek during searches. Users are typically allowed to choose from three setting levels ranging from unfiltered to highly filtered. These filters tend to focus primarily on pornography and adult content. This feature may provide an important addition to a parent's Internet management as it can provide filtering of search, which is often not provided by commercial filtering products. Some "safe search engine" filters are not filters at all, however. Some, such as Yahoo! for Kids (formerly known as Yahooligans), offer only preapproved sites in their site pool. The

search engine filters may not block inappropriate images or videos, however, unless the textual description of these media includes keywords identifying them as problematic content.

- **Web Portals for Kids (or "Walled Gardens")**: Many websites restrict content to only that which is appropriate for children. These sites may let kids search for content without the risk of stumbling upon adult-oriented material and help them discover new images, videos, and other kid-appropriate content. They may also help direct children to information and sites that are educational and enriching. In essence, these search portals are massive white lists of acceptable sites and content that has been pre-screened to ensure that they are appropriate for young web surfers. They also provide a safe Web experience for non-readers. To be effective, parental supervision or filtering or other technical tool may be needed to ensure that a child does not navigate away from such websites. One downside of using such services is that a lot of wonderful material available on the World Wide Web might be missed, and children will not be able to discover new sites, content, and games that might have been missed in the massive amount of unscreened Internet content. But many parents may be willing to make that trade-off since they desire greater protection of their children from potentially objectionable content. Concerns have been raised about how appropriate content is selected, how the service handles rapidly-changing URLs and content on previously trustworthy sites, and lack of consistency. Transparency of standards and processes is an important factor in allowing parents to know which site, portal or product to trust.

- **Device / Set-Top Box Embedded Controls**: Many providers of consumer electronics and digital devices now "bake-in" parental control technologies into their hardware. Many video game consoles, DVD players, wireless routers, mobile media devices and phones, cable and satellite set-top boxes, and many other digital devices now include parental control tools. These embedded safety and security tools include: content filtering and screening technologies, time management controls, monitoring capabilities, and blocking tools to restrict access to the web or other users (through "buddy lists"). The primary weakness of these tools is a lack of consistency across platforms; not every device possesses identical capabilities since they are tailored to the needs of specific customers. In addition, using multiple systems and terminologies may be confusing to parents. While widespread protections are not generally available yet in the mobile phone market, parental control products are emerging that allow parents to supervise and control both web and telephone usage on their child's phone.

- **Rating and Labeling schemes**: Several of the technologies mentioned above rely on rating and labeling schemes to trigger filtering mechanisms. Official industry ratings systems—such as the Motion Picture Association of America (MPAA), Entertainment Software Rating Board (ESRB), and Recording Industry Association of America (RIAA) systems – are particularly helpful to technology providers, since they facilitate easier content screening/blocking. Labeling user-generated content is much more challenging, but many websites encourage "community policing" and labeling efforts that let users "tag and flag" the content posted by others in their online community. Site providers or tool makers can then use those "crowdsourcing" efforts to power screening mechanisms. Of course, some sites supplement this with real-time content review, such as porn image detection and review of content textual tags.

HOW WELL IS THE PARENTAL CONTROLS MARKETPLACE FUNCTIONING? WHAT WORKS PARTICULARLY WELL? CONVERSELY, WHAT ISN'T WORKING SO WELL?

Summary

The general consensus from the experts we heard from and from the comments offered by OSTWG members suggested the parental controls marketplace is functioning fairly well for users who understand basic computer security, but that more could be done to improve awareness and usage of existing tools while also striving to improve the tools themselves.

In particular, ease of use is a major concern for some. In addition, several speakers before the task force stressed the continuing challenges associated with the rapid pace of technological change in the Digital Age. User-generated content also presents new challenges for parental control technologies since "amateur" content is ubiquitously available and yet typically not rated or as easy to filter or block (although some filters can block user-generated-content sites entirely).

Discussion

What follows is a synthesis of some of the comments offered by task force members regarding what is and is not working well in this arena currently.

Upsides

Like most areas of the consumer software market, parental controls enjoy robust competition from many companies targeting the same, relatively small market: parents with children old enough to use a computer but young enough to require supervision (although some parents believe all minors require supervision in their online activities).

Software development for the business / enterprise / school segment of the market looking for filtering and monitoring software eventually trickled down to the consumer looking for home solutions, this time targeting parents and their children rather than corporate IT, employees, and students. This competitive market manifests itself in multiple ways, some good and some bad. The upside of this competition is that many products are available, allowing parents to choose software or services that fit their specific needs. That need may boil down to monitoring, filtering and blocking, or some combination of both.

Many major Internet service providers offer some type of parental controls for free. Along the same lines, many broadband providers integrate parental controls into their products and work to educate their customers about their availability and usage.

Some of these basic parental control offerings may have additional value as digital training wheels for kids. One respondent noted that a control as simple as time restriction for Internet usage for younger children not only laid the foundation of boundaries for the child but also established a comfort level for the parent with the feature. As the child grows older, the parent may be more willing to remove the training wheels, so to speak, and ease their children into other forms of media content or communications platforms – and then use a different set of tools to address concerns.

Websites, service providers, toolmakers, and rating organizations have also adapted to changing market conditions. Rating and labeling systems are evolving to account for new forms of content or expression, and have generally become more granular over time, although they are always in a race with evolving technologies and forms of content. Filtering systems are still developing for cell phones with Internet access, portable game players such as PSP, or iPods. The mobile "app" market has

exploded in recent years and the industry is seeking ways to offer rating schemes and new parents controls, although in a somewhat less coordinated way than other industry sectors. Nonetheless, many of the most popular wireless devices now allow application restriction by rating at the phone's operating system level.

Privacy controls are also becoming an accepted – even required – component of online communities and services. As users have demanded more control of their personal data, sites and service providers have adapted to include privacy and data security controls.

Finally, the diversity of products available to parents suggests that there are many kinds of tools available from which parents can choose. It would seem that parents have many different opportunities to utilize various technologies and various approaches to safeguarding their children's media consumption and online experiences.

Downsides

The inverse effect of the product diversity mentioned above is the confusion it creates for the consumer. In this market, that confusion could be exacerbated by the possibility that some consumers are already uncomfortable with the technologies they are evaluating. Some many find it difficult to choose a product, install or activate a program, and maintain it effectively.

Without industry coordination at a higher level, the competing claims made by several products further muddle matters when directed at consumers who may lack the ability or time to sort through competing claims and capabilities. One step suggested by several task force members would be to develop, at the industry level, a centralized website where parents can evaluate parental control solutions using common metrics. For instance, one product may offer filtering, one may offer blocking. To the average consumer those terms may sound interchangeable, but when stacked against each other and other products in the same category, subtle differences emerge.

The limits of technology itself also play a role. The innovative ways in which the Internet and digital technologies have evolved have not been particularly predictable and parental controls will nearly always be playing catch up. Parental control options can both under-block or over-block access to useful information leaving some parents frustrated and leading them to abandon using the product. One suggestion from a task force member was to dedicate resources to develop technologies that incorporate predicted trends. But this is an idea that, by the respondent's own admission, is an expensive and failure-prone proposition.

The Harvard study also noted that: "Filtering and monitoring technologies are . . . subject to circumvention by minors – especially older minors – who are often more computer literate than their parents and who access the Internet increasingly from multiple devices and venues.... Home filters also cannot protect at-risk minors who live in unsafe households or do not have parents who are actively involved in their lives."[50]

Some task force members were concerned about the narrow focus of the industry on the home PC relative to other devices or methods of accessing digital content. In the last few years, wireless access points have exploded, with nearly any device imaginable becoming wirelessly connected to the Internet, from mobile phones to video game consoles to refrigerators. Many worry that the scope

50 Internet Safety Technical Task Force, *Enhancing Child Safety & Online Technologies: Final Report of the Internet Safety Technical Task Force to the Multi-State Working Group on Social Networking of State Attorneys General of the United States,* Dec. 31, 2008, at 153, http://cyber.law.harvard.edu/pubrelease/isttf.

of available software for new devices or platforms is too narrow or that parents are not adequately informed about how to take advantage of existing solutions.

One thing that the current parental controls technologies handle less well is Web 2.0 or user-produced content (including content created by kids). This affects older children who frequent social network sites in particular, since current software solutions typically only offer a pass / fail (allow or block) option when confronted with something like the dynamic content on a social network site. That binary choice may be undesirable, and potentially unworkable, for parents of increasingly social teens.

Lack of sufficient product integration is another area where some argued there was room for improvement. Some respondents note that parental control tools sometimes appear to be tacked on as an afterthought at the end of a product's design process. Parents are sometimes unaware of the options and how to locate and activate them on any given service or product. A unified, ground-up approach in which parental controls are a core piece of the product's construction would be welcome. Of course, even if they are "tacked on as an afterthought," many of those tools can still be quite effective.

Finally, the very term "parental controls" is problematic to some. Given the various methods by which these parental control software products work, more specificity could be warranted to reduce confusion on the part of parents. For example, blocking software and monitoring software would probably fall under the label of "parental controls" but each does something very different. Were a parent to choose one over the other blindly, there may be a false sense of security that harmful content is being blocked from the machine when that is not always the case. As a component of the call for more education, a shift from a catch-all term for a diverse spectrum of software could be appropriate.

HOW DO YOU MEASURE EFFECTIVENESS IN THIS CONTEXT?

Summary

Measuring effectiveness and success in this arena remains a controversial topic. The experts on our task force and those presenting at our meetings had varying definitions and metrics regarding the effectiveness of parental control technologies and rating and labeling systems. And the issue is complicated by the nature of the marketplace, where the available technologies, content, and parental demand and concerns are always in a state of flux.

Discussion

Measuring effectiveness requires more than simply collecting and tallying data, because determining what is "effective" necessarily involves some value judgments. Some online safety task forces have attempted to incorporate evaluations of various approaches and technologies.[51] The OSTWG task force did not possess the resources to conduct a similar review, and, as noted above, our efforts were limited by the confines of the Paperwork Reduction Act.

However, to the extent evaluation of effectiveness is conducted by future task forces or working groups, several OSTWG respondents offered up potential criteria for evaluating effectiveness. Among them:

51 See: Computer Science and Telecommunications Board, National Research Council, *Youth, Pornography and the Internet* (Washington, DC: National Academy Press, 2002), www.nap.edu/html/youth_internet and Internet Safety Technical Task Force, Enhancing Child Safety & Online Technologies: Final Report of the Internet Safety Technical Task Force to the Multi-State Working Group on Social Networking of State Attorneys General of the United States, Dec. 31, 2008, http://cyber.law.harvard.edu/pubrelease/isttf.

- Ease by which parents can find products and services they need
- Efficacy of each tool to do what it claims to do
- Likelihood that parents to effectively deploy a product to address a perceived need
- Sufficient labeling of minimum system requirements to run a product
- Ability of parents to understand how a product interacts both with the machine and with users
- Flexibility of a product to deal with the progressing age and skills of the child
- Disruption that products cause to acceptable Internet activities
- The likelihood that use of the parental controls were abandoned for being ineffective, too hard or not fitting the family's needs

Another factor to consider, as discussed above, is that measuring the uptake of parental control software may not provide a complete picture of parental involvement in their children's Internet usage. Several respondents noted that many families choose many methods other than technology to monitor or control their children's media and Internet usage. Statistics regarding the number of students who learn about Internet safety at school would also be a valuable metric in assessing the effectiveness of strategies designed to keep children safe online.

WHAT COULD BE DONE TO GENERATE GREATER AWARENESS OR UPTAKE OF PARENTAL CONTROLS OR CHILD PROTECTION TECHNOLOGIES?

Summary

There was a great deal of agreement among the experts we heard from as well as the OSTWG members that industry, researchers, government, and other organizations can take more steps to expand awareness about parental empowerment technologies. Comments along these lines were typically grouped into three sets of recommendations: (1) Engaging parents and kids in greater conversation; (2) Increasing general education and awareness efforts and campaigns; while (3) Improving the quality and ease-of-use of the tools themselves.

Discussion

Respondents were generally in agreement about the major requirements to increase awareness, and potentially uptake, of parental software. First, engage the consumer. Ask parents what they need and what they are looking for from a parental software product and manage the false expectation that once the parent installs this product on their home computer their child is now "safe" on the Internet. As part of this process, also engage children. Find out what they are using the Internet for, at progressive age levels, and determine how products can help enforce parental boundaries while not detracting from the usefulness of allowed websites. Some respondents suggested highlighting the positive content that these tools will allow children to see, rather than emphasizing all of the questionable content the tools will keep out; however, others felt that parents may not sufficiently understand the risks and underestimate the need for supervision of children online. Along similar lines, emphasize that parental software is just one tool in a parent's hand, not a replacement for supervision and active participation in their children's online experiences.

Second, educate the consumer. Reach out via the media with positive campaigns emphasizing what properly supervised children can accomplish academically and socially with Internet access. High-volume Public Service Announcements are typically effective at creating awareness, and industry best-practice guidelines would help standardize what parents can come to expect from parental software

and reduce consumer confusion. Some respondents suggested that legislation earmarking funds for consumer education and digital literacy campaigns would be helpful, and others suggested that devices used to connect to the Internet (such as game consoles) could come with highly visible labels informing parents that the device could be used to access the Web.

HOW DO YOU FEEL ABOUT DEFAULT SETTINGS? SHOULD MEDIA AND TECHNOLOGY PROVIDERS ESTABLISH MORE RESTRICTIVE DEFAULTS FOR THEIR PRODUCTS AND SERVICES? SHOULD THE GOVERNMENT MANDATE OR "NUDGE" PROVIDERS TO SET DEFAULTS MORE RESTRICTIVELY?

Summary

Default settings—or how parental controls are configured "out-of-the-box" by vendors or website operators—are another controversial topic. The experts and OSTWG members we heard from had differing views on how parental software defaults should be set and who should set them. And because there is such a broad diversity of sites, services, content, and applications that must be considered, the wisdom of default settings can only really be considered by narrowing the scope of focus.

Generally speaking, however, most agreed that the government should not be in charge of establishing the defaults. The controversy came instead from the question of whether content creators and distributors should voluntarily set defaults more restrictively and then let parents "opt-out" of those settings. Or, alternatively, if they should simply provide clear and unambiguous notice of the parental empowerment technologies available and let parents "opt-in." Several participants, however, stressed that setting defaults too restrictively could create confusion or hamper the user experience unnecessarily. Some participants believe that setting reasonable defaults (with notice that more and less restrictive options are available) would be helpful.

Discussion

Respondents generally agreed on two ideas:

1. Default settings should be given careful consideration before shipping a product because they typically go unchanged after the fact; and,
2. Government intervention to establish default settings is undesirable for several reasons.

To the first point, default settings should be carefully considered during the product design phase, and a product should be evaluated based heavily on how it performs out-of-the-box, given that most consumers do not alter the default settings on technology products. To mitigate this behavior, there were suggestions such as ensuring that products were set to "non-stealth" mode by default or that they would launch with a set-up wizard to guide parents through the choices that are available to them, rather than keeping the default settings buried in a menu that some parents may have difficulty finding.

Some voiced the opinion that since settings can ultimately be changed, why not simply default them to the most restrictive possible? Others countered that if a product is too restrictive out of the box it would block content to the point where many would complain that the product is "broken" and the potential for abandonment would increase. A median suggestion was to invest in research to determine a level of restriction that is neither too loose nor too restrictive, and combine default settings with education about changing the defaults.

Several respondents echoed similar opposition to government intervention in mandating the

restrictiveness of default settings. Government-mandated default settings, which would serve to restrict access to information, may raise First Amendment concerns. Another argument against mandated defaults is the inability of government to act quickly enough to keep up with the speed at which the Internet and digital technologies evolve. What may be considered a threat today may be benign tomorrow or vice versa, and if the industry were handcuffed by a requirement for rigid settings, the likelihood of a product's adoption and ultimately control tool companies' ability to do business would suffer.

One suggested compromise would be an agile, evolving set of industry best practices developed through collaboration between industry, NGOs, and government, which could serve as common ground while also adapting to changes in the landscape.

WHAT IS THE PROPER ROLE FOR GOVERNMENT IN THIS CONTEXT?

Summary
The OSTWG members and experts we heard from offered a smorgasbord of useful suggestions regarding how government could help in this area. Generally speaking, however, most were not keen on the government playing a greater regulatory role. Instead, education, funding, and empowerment strategies tended to be at the heart of most of the recommendations.

Discussion
Funding and a light touch when it comes to any type of mandate was the nearly universal reply from panelists to this question. Among the endeavors that would benefit from government funding include: digital literacy programs, public service announcements, and public school curriculum.

Tax incentives for companies to encourage product innovation or to bring themselves into voluntary compliance with best practice guidelines was one suggestion, as was additional law enforcement funding earmarked for Internet-related matters.

Other suggestions included adoption of a set of national goals in the space of online child safety to guide the industry, along with funding to engage the public health sector in the area of at-risk youth in the online setting.

WHAT SORT OF ADDITIONAL STUDIES OR RESEARCH WOULD BE USEFUL GOING FORWARD? WHAT QUESTIONS DESERVE MORE STUDY?

Summary
Task force members and the experts we heard from all agreed that more research would be helpful in determining what does and does not work in this area. Several experts spoke of the need for a better "gap analysis" to determine the tools and approaches needed to address existing or emerging concerns. While the Pew Institute and others devote substantial resources to these studies on an ongoing basis,[52] there may be need to study issues with a more precise focus.

Discussion
Among the suggested areas of additional study:

- Technology adoption and use in the home by age of child
- Technology adoption and use in the context of the US educational system

52 See supra note 3, for instance.

- Parental control software adoption and use in the home by age of child
- What the major impediments are for parents who don't use parental controls
- Parents' goals in using technology tools to help protect, supervise, and monitor their children by age of child, and how they differ with those of a child.
- Long-term effects of differing methods of parental supervision and communication with and without using parental control software technology by age of child
- Parental concerns and awareness of online safety risks
- Impartial benchmarking and testing of parental control software
- Parental control software products currently under development
- Identification of online risks for youth by priority and age
- Short and long-term effects of encounters with age-inappropriate or potentially offensive content online and other risky behavior
- Short and long-term effect of education programs on the mitigation of risks that youth face online
- Unique safety concerns with "at-risk" youth in an online setting and how best to address them

GENERAL CONCLUSIONS & RECOMMENDATIONS REGARDING PARENTAL CONTROL TECHNOLOGIES

Generally onsistent with what other online safety task forces have found, with regard to parental controls technologies, the majority generally concluded that:

1. **There is no single "silver-bullet" solution or technological "quick-fix"** to child safety concerns. That is especially the case in light of the rapid pace of change in the digital world.
2. **Empowering parents and guardians with a diverse array of tools**, however, can help families, caretakers, and schools to better monitor or control online content and communications.
3. Technological 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.
4. The best technical control measures are those that work in tandem with educational strategies, parental involvement and approaches to better guide and mentor children to make wise choices. Thus, **technical solutions can supplement, but can never supplant, the educational and mentoring role**.
5. **Products and services need to be designed with the families' needs in mind,** allowing parents to use the right settings and the right tools for their need and adapt to changing needs. Parental control technologies **have to be easy to use, accessible, flexible, and comprehensible for the typical parent.** They need to provide different features for the varying needs of all the children in the household.
6. **Industry should continue to formulate and refine best practices and self-regulatory systems** to empower users with more information and tools so they can make appropriate decisions for themselves and their families. And those best practices,

which may take the form of an industry code of conduct or default control settings, should constantly be refined to take into account new social concerns, cultural norms, and technological developments.

7. **Government should avoid inflexible, top-down technological mandates**. Instead, policymakers should focus on encouraging collaborative, multifaceted, multi-stakeholder initiatives and approaches to enhance online safety.
8. **Additional resources for education** and awareness-building efforts are absolutely crucial.
9. **We must engage our youth in constant dialogue** and always be willing to talk to them about difficult issues, challenges, or content they face online.

SPECIFIC RECOMMENDATIONS ON PARENTAL CONTROL TECHNOLOGIES

Content creators, digital device providers, website administrators, and network providers should:

1. **Engage in ongoing awareness-building efforts**: The more education and awareness-building the better. Improved product descriptions, tutorials, and other forms of user assistance are vitally important.
2. **Promote greater transparency**: Users/parents should be given a clear understanding of what sort of content and information they will come in contact with when they or their children use certain media products or visit certain websites and use features allowing them to communicate with third parties or share information.
3. **Parental empowerment technologies and options should be included in new offerings whenever possible**: "Safety by design" should be encouraged and companies, sites, and services should "bake in" safety tools and settings whenever and wherever possible. Greater industry collaboration and common approaches are also encouraged.
4. **Enable and promote "community policing"**: Social networking sites and other sites that host user-generated content should utilize, improve, and expand "community policing" capabilities. Reporting mechanisms should be established and refined to ensure problems are dealt in a timely fashion.

PARENTAL CONTROLS TECHNOLOGY SUBCOMMITTEE: ADDENDUM A

SURVEY OF OSTWG MEMBERS AND PRESENTERS ON THE STATE OF PARENTAL CONTROLS & CHILD PROTECTION TECHNOLOGY

OSTWG members and the experts we heard from were asked to comment on a variety of questions that the task force was pondering, including:

1. Generally speaking, how well do you think the parental controls **marketplace** (broadly-defined) is functioning? What works particularly well? Conversely, what isn't working so well?
2. How do you measure **effectiveness** in this context?
3. What could be done to generate greater **awareness** or uptake of parental controls or child protection technologies?
4. How do you feel about **default settings**? Should media and technology providers establish more restrictive defaults for their products and services? Should the government mandate or "nudge" providers to set defaults more restrictively.
5. What is the proper **role for government** in this context?
6. What sort of **additional studies / research** would be useful going forward? What questions deserve more study?

A sampling of some thoughts and findings about these six questions follows.

HOW WELL IS THE PARENTAL CONTROLS MARKETPLACE FUNCTIONING? WHAT WORKS PARTICULARLY WELL? CONVERSELY, WHAT ISN'T WORKING SO WELL?

Upsides (or What's Working Well)

- "The parental controls marketplace is, like many markets, a collection of companies vying for a relatively small audience (e.g., parents with children of a specific age group). In one sense, this creates healthy competition among the players which generally produces better results in terms of feature sets than regulated markets. On the other hand, it can be confusing for a parent to determine *which* tools are the best for their specific situations. It can sometimes be difficult to sift through the marketing hype to make a decision that suits your own needs and parenting styles. Also, there isn't a 'magic bullet' solution that covers all aspects of parental controls in all situations." – ***Holly Hawkins, AOL***
- "I do think that the parental controls marketplace offers a fairly wide range of tools that can be used to enhance child online safety – whether integrated features of online products and services or as standalone solutions." – ***Elizabeth Banker, Yahoo***
- "There are many product choices and the technology is quickly advancing—seems like the market is functioning well. The industry is increasingly competing on privacy and security, and improvements in these areas spillover in the child context. However,

markets function best when consumers have a high degree of product awareness and education. Unfortunately, there's more to be done to make parents more aware of the technology tools they have at their disposal, and how best to use them for their desired effect." – ***Braden Cox, NetChoice***

- "USTelecom believes the parental control marketplace is functioning extremely well. What is working particularly well is that parents today have numerous choices and tools to choose from in ensuring their children have access to a safe media environment. Additionally, many wireline broadband providers are actively educating their customers on the availability and benefits of tools available through their online and/or video offerings (*e.g.*, DVRs, Parental Control online tools, etc.). Many wireline broadband providers are also directing their customers to additional, third-party resources for keeping their kids safe online." – ***Kevin Rupy, USTelecom***
- "The marketplace *per se* is working well. There appears to be no shortage of software solutions, and most major ISPs offer complimentary parental controls packages to their subscribers." – ***Rob Stoddard, National Cable & Telecommunications Association***
- "One feature of parental controls we find used regularly is internet access time limits for the younger children. Including the software for free with a service makes the choice easier for parents to try. Parents who have started in the early years getting involved in their children's online activities and attempt to keep up with the technology find it easier to be a part of the child's online activities in older years." – ***Jay Opperman, Comcast***
- "Ning has… found that giving users (parents AND children) the opportunity to police or 'govern' their own communities by providing them with the appropriate community management tools to do so and educating them on how to use them is extremely powerful. It is very effective when someone is empowered to take ownership of their community – they want the community to be safe. The community will police itself when they feel that they are actually a part of it." – ***Jill Nissen, Ning***
- "We want a variety of solutions in the marketplace because there is such a huge diversity in user needs. It is not clear to me that a significant percentage of parents are asking for parental control technology that does not exist in the marketplace." – ***Brian Markwalter, CEA***
- "Wireless carriers offer a plethora of parental empowerment tools, including but not limited to, content filters, calling and text limits, camera function limits, parental notifications, pre-approved calls, and purchase limitations. Wireless carriers also voluntarily adhere to CTIA's Carrier Content Classification and Internet Access Guidelines. Wireless manufacturers offer a variety of built-in parental empowerment tools, such as password protected function and feature limits. In response to the burgeoning wireless applications ("apps") market, manufacturers are also developing or offering content rating and filtering tools. Third party vendors offer a variety of downloadable parental empowerment tools including device monitoring, parental notifications and content filters." – ***Dane Snowden, CTIA***
- "Game consoles and handheld devices are highly effective at blocking by ESRB rating. Certain game consoles are highly effective at providing a parent with the ability to manage whom their children can play with online, and in some cases when and for how long. Many offer restrictions on access to online content and offer helpful guides on how these settings can best meet a parent's individual needs. That being said, no single tool or set of tools will solve the "digital divide" between those households who care

about being proactive about Internet safety and those who don't." – ***Patricia Vance, ESRB***

- While there is a great deal of confusion around parental controls, there are some things that are working well. There are a variety of tools that are free or affordable. Parents, once they know what to look for, can find the right product to fit their needs and tech skill levels. The industry has been very responsive and better approaches, features and technologies are made available frequently. The industry and providers often combine educational tips with their parental controls which makes the tools relevant and helps parents make the right choices. Privacy settings are now accepted practices and users can typically block strangers and known harassers from being able to communicate with them online. Unlike the early days of parental controls in 1995, parents can find what they need, often for free, through a simple search online or by viewing their provider's help or safety pages. - ***Parry Aftab, WiredSafety***

- "What makes the parental control approach work is the diversity of tools available, both in terms of what the tools do (monitor, filter, etc.) and in terms of what types of content the tools allow parents to control. Families that want very strict controls will find options, as will families that instead seek looser controls that only address the most extreme content. And as children grow up, the tools available can evolve and grow with them. And more broadly, there is significant competition in the marketplace." ***– John Morris, CDT***

Downsides (or What's Not Working So Well)

- "There is no industry coordination, everyone is doing their own thing. There are vastly overblown claims, parents don't know which to believe. There is no central site/service to highlight all of them and show the differences." – ***Parry Aftab, Wired Safety***
- "The potential dangers our children face through their use of technology is changing faster than software makers can keep up. Much like the malware marketplace, vendors are always a step behind latest threats. The best parental controls providers can do is to anticipate how kids will be using technology in the future, and take risks on investing in products to meet that future need." – ***Holly Hawkins, AOL***
- "The parental controls marketplace functions well under some very specific and limited circumstances, but it is inadequate in other essential areas. While we recognize many improvements in products over the last five years, most parents remain overwhelmed with the task of managing their family's Internet experience, particularly parents with older youth. The parental controls marketplace works well for managing content for young children who use a limited number of connected devices. Where iKeepSafe envisions improvements is in the protection for older children who want to participate in the web community. It's very hard for parents to manage the Internet experience of older youth when they need to be on sites that cannot be filtered adequately. One primary, glaring hole in the parental controls marketplace is the lack of a plug-and-play, pre-filtered Internet service, suitable and affordable for consumers, where filtering occurs outside and independent of the home computer. Many products exist that adequately—not perfectly—filter content unsuitable for children. Another hole in the marketplace is in the parental controls for Web content available through cell phones. While many providers offer filtering and monitoring software, most parents either don't know they exist or don't know how to use them." – ***Marsali Hancock, iKeepSafe***

- The parental controls market does not effectively manage Web 2.0 content. Kids want to be where they can share content: Norton identified YouTube, Facebook and Google as the top three searches for kids. Social networking, virtual worlds, gaming, and media sites where user-generated content is uploaded are difficult to filter by individual user. Within some of these sites, improvements have been made to regulate content by allowing users to flag inappropriate content. Even with these improvements, parents still struggle to provide a managed Internet experience for children in these sites. Many parents feel that the only secure way to block inappropriate content in these venues is to block the sites entirely. iKeepSafe does not see this as a realistic solution. – ***Marsali Hancock, iKeepSafe***
- "Certainly, there is a plethora of products. The sheer quantity of competing products may actually contribute to the despair parents feel when trying to make intelligent decisions. Some kinds of uniform standards of measurement and required disclosures would be extremely helpful. Although many of these parental control options offer some meaningful protections, none are sufficient and it would be misleading to suggest the only difficulty is choosing among existing offerings. "The most commonly reiterated concern of members of OSTWG was that parents are not satisfied with what they perceive to be the options. Of course, this problem may be mitigated with a coordinated education effort, but we did not begin to formulate a feasible scheme for getting the information to parents." ***– Ralph Yarro, Think Atomic***
- "Industry does provide some parental controls, and filtering, but they could make it much easier to find these features on their pages and much easier for parents to understand and use. While they may provide it, parent controls and child safety need to be a top priority. One of the challenges with the Internet is that there is currently no way to separate out inappropriate content from content that is appropriate for children. Filters can be used and are certainly helpful, but they're not child-proof. Many parents know they should be using filters, but are not for various reasons. ISPs should have a duty to protect children from the potential harmful effects of the internet." – ***Jeremy Geigle, Arizona Family Council***
- "Many parents are not aware of the products that are available. There is no standardization among products in their use, so "parental controls" on one system operate differently than parental controls on another system, and makes it much more difficult for users." – ***Hedda Litwin, NAAG***
- "Parental controls and utilities are only effective to any degree when they are being used. That initial and paramount hurdle is one that has not yet been effectively overcome. Eventually this problem will resolve itself as people who grew up using computers and the Internet become parents themselves, but in the interim more outreach to parents would be welcomed. As important as the message itself is, the medium through which it is delivered is crucial to success. Often this message is delivered through the Internet itself, perhaps through safety oriented organizations. This can be an effective however the parent most in need of information is the parent who likely doesn't even know they need it. Putting the information where parents can easily access it, be it via television, print, or radio, would be a measure that could help soften the narrowing gap between once intimidating technology and a parent's participation in their child's internet activity." – **Hemanshu Nigam, MySpace**
- "Many parents are still not aware of the various products out there. Better adoption appears to be when incorporated for free into a product or part of the product offering

from the start (i.e. the various granular privacy and safety options available on sites such as Ning, Facebook, MySpace, etc.)." – ***Jill Nissen, Ning***

- "A parent's decision not to employ parental controls in his or her home, be it proactive or passive, may be due to a variety of reasons, including but not limited to: 1) lack of awareness of the tools available; (2) lack of concern or awareness about the risks associated with his/her child's use of the Internet; (3) lack of sophistication in many tools to account for individual tastes, values, concerns or age of child -- and for those tools that are more sophisticated, lack of ability or interest in spending the time and effort to set them up; and (4) inaccessibility of the device in the child's possession or bedroom. We need to better understand what motivates a parent to use such tools and why many don't use them today." – ***Patricia Vance, ESRB***
- "[M]ore work must be done to develop and implement parental controls for social media applications across all platforms." – ***Rob Stoddard, National Cable & Telecommunications Association***
- "Probably adequate but it could be better…sometimes it feels these are bolt on capabilities versus something that is thought of as core to the service." – ***Jay Opperman, Comcast***
- "The marketplace is a bit confusing. For example, even the term 'parental controls' is a catch-all encompasses many different kinds of software functions that aren't included in every software package. There are different functions and expectations for safety using different software tools—filters, blocking, monitoring, etc.. This can cause confusion for parents." – ***Michael Kaiser, National Cyber Security Alliance***
- "As technologies evolve and new ones emerge, the tool makers will necessarily have to work to keep up. Most tools regularly release updates and new filtering lists, but no tool will ever be perfect. But that is true of the vast majority of child safety tools in our society – from car seats to bike helmets." – ***John Morris, CDT***

HOW DO YOU MEASURE EFFECTIVENESS IN THIS CONTEXT?

- "The base measures of parental controls effectiveness are adoption, tenure, and satisfaction. If parents aren't adopting, using, and happy with their chosen parental controls product, then it is not effective. Factors influencing parental controls product success include ease of use (install, set up, configurations), breadth of features, use across devices (single PC, network, mobile devices, etc.), and time commitment necessary from parent to manage controls. Another factor is the relevance of the product to the age of the child in question. A child of 5-7 is going to use technology much differently than a teenager, and tools that are effective for one are not necessarily effective for the other." – ***Holly Hawkins, AOL***
- "In terms of effectiveness of such tools, it appears that there is still some resistance to wide-spread use of such tools and that the gap may be due to a lack of knowledge on the part of parents and other responsible adults or a lack of engagement in kids and teens online behaviors. Lack of use of even really great tools that do exactly as promised should probably be considered when looking at the status of such tools and what they currently add to the child safety effort. However, I do not think that lack of use should be taken as a reflection on whether or not the technology is where it needs to be. It's kind of like a seatbelt only working if you buckle it – that's not a flaw with the seatbelt." – ***Elizabeth Banker, Yahoo***

- "You have to ask parents. Is it working the way it is? (The answer is a resounding "no!" for the thousands of parents I speak with each month.) So, we have to ask them about their needs. When products are too complicated for parents to use effectively, they abandon them. Many product providers shoot from the hip. They address the needs of one demographic group, ignoring others, are very value-based or overly-complicated to avoid being value-based, and make assumptions about parents as a whole, just because they have children themselves. They don't know their markets as well as they should and have a large failure rate." – ***Parry Aftab, Wired Safety***
- "We measure effectiveness based on several factors: (1) How likely are parents to find the product/service? (2) How likely are parents to have the necessary skills to implement the product/service effectively at home? (3) How often is the parent's routine disrupted by the service? How many times a day does a child request access to a legitimate site because of parental control interference? Does the product slow or impede the online experience for the adults in the home? Does the machine used in the home have sufficient memory to run the product effectively? (4) Can the parent meaningfully engage in what the child is doing online in terms of content viewed, contact with other users, and conduct within Web communities? Can parents effectively manage the Internet experience as the child ages, ramping them into responsible digital citizenship?" – ***Marsali Hancock, iKeepSafe***
- "This is a difficult question. Since for each type of software there are different measures, we need to establish effectiveness by type (blocking, filtering, monitoring, etc). A stronger consensus around what effectiveness means would be helpful as well. One clear measure is consumer satisfaction. Does the product, in their experience, actually do what it promises, and do parents feel that their children are safer as a result." – ***Michael Kaiser, National Cyber Security Alliance***
- "Two prongs to measuring effectiveness. (1) The first is to measure the number of young people in our school systems that are being taught internet safety. Just because they know about the dangers doesn't mean that they won't intentionally place themselves in danger, but it at least gives us a quantifiable measurement of those being taught about the danger. (2) Gauge the number of young people (and adults) who are successfully using internet safety education to avoid inappropriate content." – ***Jeremy Geigle, Arizona Family Council***
- "It is critical to differentiate between a measure of effectiveness for a given product, such as a filtering program, and a measure of effectiveness for the entire concept of user or parental empowerment as an approach to online child safety. With regard to individual products, the federal judge who decided the COPA litigation received extensive evidence from expert witnesses, and found that the leading filtering tools were highly effective at blocking out unwanted sexual content – far more effective than the COPA law being challenged in that case. The filtering tools were able to block 90% of more of such content. Looking more broadly, however, the question of societal uptake of filtering tools is *not*, in my view, a good measure of the effectiveness of the user empowerment approach to online safety. Many families choose methods other than technology to supervise and guide their children's online experience. More effort to promote awareness of technical tools is certainly desirable, but the fact that many families do not install filtering software does not indicate that user empowerment is not an appropriate approach to online child safety." – ***John Morris, CDT***

- "Data of consumer awareness and attitudes toward available control tools and services developed by an independent and reputable organization. Independent non-governmental review bodies to determine that available content tools meet consumer expectations." **– *Dane Snowden, CTIA***
- "Measure usage of the controls. Surveys of satisfaction with the parental control tools." – ***Hedda Litwin, NAAG***
- "There is a need for more research on consumer awareness and use of the broad array of parental controls and tools available today, and particularly to gain insight into *why* those parents who are aware of parental controls choose not to use them. We also need to better understand consumer satisfaction with the tools in use, by reviewing consumer feedback and conducting consumer research. Moreover, the efficacy of tools to do what manufacturers say they do should be evaluated." – ***Patricia Vance, ESRB***
- "Public opinion polling could be utilized to measure awareness, usage, and effectiveness of parental controls. In addition, consultation with ISPs, internet companies, law enforcement officials, and other stakeholders, to identify potential reporting and tracking mechanisms for the volume and trending of concerns or complaints, might be useful." **– *Rob Stoddard, National Cable & Telecommunications Association***

WHAT COULD BE DONE TO GENERATE GREATER AWARENESS OR UPTAKE OF PARENTAL CONTROLS OR CHILD PROTECTION TECHNOLOGIES?

Importance of Talking to Parents & Children / Encouraging Constant Engagement

- "Start with the parents. Ask them what they need and make it easy for them to use the products, make them relevant and not overwhelming. Manage expectations. They often think they can set it and leave it. But effective tools require tweaking and rethinking, as well as moving the bar when the kids become older and better able to protect themselves. Also, get kids and teens involved." – ***Parry Aftab, Wired Safety***
- "Talk to parents AND children. One thing that Ning has done is really engage our members and Network Creators and get their input on what is and what is not working with the tools that they have to control their privacy and safety and moderate their social networks." – ***Jill Nissen, Ning***
- "I think the continued struggle is how to get parents and other adults more engaged in what kids do online. Frankly with the proper level of engagement, such as parents who talk to their kids about what is and is not okay to do on Facebook, the tools are probably a lot less important. I'm not sure exactly how to do this, but we have seen several fairly negative campaigns designed to motivate parents with fear and I think trying something more positive may reach the audience who has not responded to fear-based messaging." – ***Elizabeth Banker, Yahoo***
- "Software is no substitute for supervision by a parent or guardian or for open communication with children and teens. Because parents cannot always be present when their child is online, filtering and monitoring software can be a valuable tool, but it cannot guard a child from potential risks that exist online. It is always important to remember that an Internet filter is a tool and is no substitute for your supervision or for regular communication with your children or teens." – ***John Shehan, NCMEC***

General Education / Awareness-Building Efforts

- "Get the word out – there is still a lot of misinformation about the technologies and what they can and can't do. Be positive in conveying the real message and debunk the urban legends." – ***Parry Aftab, Wired Safety***
- "A national media literacy campaign targeting different audiences (i.e., younger kids, teens and parents/caregivers) could help to raise awareness of the tools and practical steps each can take to address Internet safety concerns. Government, NGO's, associations (ALA, PTA, etc.) and industry members can also help raise awareness and distribute educational materials on digital literacy." – ***Patricia Vance, ESRB***
- "A national campaign by the Ad Council might help generate more awareness to parents that these types of products are available – and often at low or no cost from their ISPs. Internet service providers could also do more to highlight the parental control products that they have available to their users, and how the users can benefit from using the products. This type of information is often buried in lower levels of their sites." – ***Holly Hawkins, AOL***
- "More focus on technology tools, less focus on fear. Encouraging technology reporters to cover parental control technologies and do occasional product reviews. Get a legislator or prominent community official to speak about parental controls. Industry needs to continue to get the word out. Educators can involve parents." – ***Braden Cox, NetChoice***
- "Cooperative efforts by industry, non-profit organizations and government are ideally suited for increasing awareness amongst consumers and parents to increase uptake of parental control technologies." – ***Kevin Rupy, USTelecom***
- "With regard to children, federal and state education policy should encourage the integration of digital literacy and responsible use courses to ensure children are positively using new technologies. With regard to parents, online safety advocates should engage on parental empowerment campaigns and encourage parents to effectively use available tools and services. With regard to industry, governmental entities and online safety advocates should continue to partner with industry to focus on specific issues and trends." ***– Dane Snowden, CTIA***
- "Companies that benefit from the internet could do more to develop, promote and market effective parental controls every time they sell their products. Awareness and education for parents is much needed to help shield children from inappropriate material online. Possibly "warning" labels on devices that access the internet, to alert parents. Local, state and national classes, online classes, online ads, public service ads, explaining the possible harms a child could encounter online and a parent's role to protect their children. Media statements, media interviews, and media blitz that bring this issue to people's attention. Industries should better promote their parental controls -- again, make them easier to access and use. If we educate the parents, it seems there would be a natural consumer demand for industries that cater to parents and online safety for children." – ***Jeremy Geigle, Arizona Family Council***
- "(1) Public service or other national campaigns to raise awareness of the various options. (2) Distribute "best practice" guides for various industries (i.e. settings for social networking sites, etc.) in schools to both teachers and children and use these guides to educate on how to stay safe online by actually using the technologies instead of just banning the use of them in schools. This should be incorporated as part of the regular

curriculum (i.e. during a computer class). (3) Make it easier for parents and children to locate and understand the various options (controls or settings) available to them on the various services (i.e. Safety Tips and Resources easily accessible, etc.). (4) Peer to peer training." – ***Jill Nissen, Ning***

- "Traditional public service campaigns - with simple messages repeated at a high frequency - are always useful. However, any consumer education initiatives on this topic should focus extensively on infiltrating online services and content and should be designed to spread virally, in order to best reach the intended audiences." – ***Rob Stoddard, National Cable & Telecommunications Association***
- "Certainly, publicity campaigns and educational efforts are admirable, but would be enormously expensive to create and coordinate at the level necessary to give a substantial number of parents the information they can effectively use." – ***Ralph Yarro, Think Atomic***

Improving the Quality of the Tools / Better Industry Coordination

- "These products tend to be all about 'no.' Parents (and the kids) need to be taught to see these as empowering, not the cyberpolice. The products should steer the users to good resources, sites and networks." – ***Parry Aftab, Wired Safety***
- "Improvement in product solutions would increase uptake. Parents do not have a viable option for providing the type of Internet that they experience at work--pre-filtered, that requires no setup from home, and that cannot be worked around by savvy kids."– ***Marsali Hancock, iKeepSafe***
- "Enclosing disclosure statements on or with any Internet facilitating product or web-enabled device that warns parents of capabilities of the product and the limited nature of optional controls may be helpful." – ***Ralph Yarro, Think Atomic***
- "The industry could come together to find ways to better characterize their products, find some common language for educating parents, establish some benchmarks for product effectiveness and quality, and establish some best practices that would be shared across the industry depending on the function of their product." – ***Michael Kaiser, National Cyber Security Alliance***
- "Apart from the aforementioned use of more traditional media to gain access to parents who don't necessarily use the World Wide Web with great skill, another strategy would be closer integration with technology at the device or operating system level. Rather than a third party piece of software that must be discovered, purchased, and installed, some companies have already found some success by integrating parental controls into devices, commonly the case with cable television boxes and digital video recorders for example. The Internet Service Provider level is another logical point to integrate some type of parental controls." – **Hemanshu Nigam, MySpace**
- "Standardize the usage of some of the parental control features so users don't have to learn new systems each time they change hardware; also one simplification manual could be used for all." – ***Hedda Litwin, NAAG***

HOW DO YOU FEEL ABOUT DEFAULT SETTINGS? SHOULD MEDIA AND TECHNOLOGY PROVIDERS ESTABLISH MORE RESTRICTIVE DEFAULTS FOR THEIR PRODUCTS AND SERVICES? SHOULD THE GOVERNMENT MANDATE OR "NUDGE" PROVIDERS SET DEFAULTS MORE RESTRICTIVELY?

- "Behavioral economics informs us that defaults matter—a lot. Most consumers will not change a preselected default setting even when given the option to do so. Media and technology providers can and should compete based on how their products perform "out-of-the-box." But industry setting the defaults is much different from governments doing so. Given that much of what is filtered, monitored, and blocked to kids is protected speech under the First Amendment, it is not appropriate for governments to decide defaults." – ***Braden Cox, NetChoice***

- "Thoughtful default settings can provide an ease of use for new users, however, since each family's situation and values can differ, settings need to be flexible to meet those needs. If defaults are set, providers should provide clear language about what those settings entail, and clear instructions on how to modify each setting. Defaults that are too restrictive can alienate users by making the Internet experience too cumbersome. For example, if a child is blocked from visiting the majority of the sites he wants to visit, then he'll complain to his parent(s) that the product doesn't "work", and the parent then becomes over burdened with having to manually manipulate settings to allow the child to have a decent experience." – ***Holly Hawkins, AOL***

- "If standardized and adopted across all major media players then more restrictive default settings may have benefits. Standardization of any level of default settings would likely be beneficial as a user would know what information they are displaying or sharing as they move from site to site without delving into their account settings, something the average user is probably not apt to spend a great amount of time doing." – **Hemanshu Nigam, MySpace**

- "Defaults should be set where parents want them. A threshold question about their concerns, values and time to commit to this can help set the right default. Best practice standards will be more effective than governmental nudging or mandates. Default should be set on "non stealth" in monitoring software, and help sites (as brought up by AOL during our session) should not be monitored. (These include child abuse reporting sites, alcohol abuse sites, etc.) – ***Parry Aftab, Wired Safety***

- "You could always force more restrictive settings…that would certainly force folks to get familiar and use the settings but from a provider perspective that is probably a negative on the user experience. This goes to the heart of the Opt In/Opt Out controversy or in other words, mandates or restrictive default settings will be perceived as taking away customers choice, even though they can change them. The better approach is to improve the tools with setup wizards, which at the initial use of the product or service requires the customer to make the choices." – ***Jay Opperman, Comcast***

- "It is not unreasonable to encourage more restrictive default settings given the concerns for protecting children and the likely gap in many parents' technical knowhow. However, parents cannot know if the default sets a parental control option that is more than window dressing. Defaults may create a false sense of security in parents who have no idea what the default means. In addition, teens, who may do most of the computer set up, can easily change the default." – ***Ralph Yarro, Think Atomic***

- "Why not have the default settings be more child protective, and let those who don't want it, opt out? Restrictive default settings will also provide some protection to the novice users." – ***Jeremy Geigle, Arizona Family Council***
- "Instead of pre-set defaults established by the government or technology providers, I think it is better to suggest certain settings for users with an explanation of why the setting is a good choice." – ***Hedda Litwin, NAAG***
- "Restrictive default settings could cause significant consumer backlash and disruption from a use-ability standpoint." – ***Patricia Vance, ESRB***
- "Any governmental mandate of a restrictive default setting would raise serious First Amendment problems, and would very likely be overturned in court. Such a mandate would reduce the flow of lawful information, and would make it harder for content providers on the "restricted" side of the default to reach their audience. Moreover, *any* default setting would be inappropriate for at least some minors – if set for older minors, then it would not protect younger minors, and if set for younger minors then it would infringe on the rights of older minors and those seeking to speak to that audience. A better approach would be to find ways to ensure that users make a choice as to their settings, rather than having the government attempt to make that choice for them." ***John Morris, CDT***
- "This is another area where industry working together could establish best practices and perhaps even some common definitions and settings that would make it easier for consumers and others to use the software 'out of the box.' The Internet changes too quickly for any entity to establish in stone what or how to set defaults. Collaborations between government and industry that includes the consumer voice could prove beneficial to establishing and evolving best practices over time." – ***Michael Kaiser, National Cyber Security Alliance***
- "In extensive conversations with content, platform, and technology providers – and based on the widely diverse composition of Internet users – we are convinced there is no one-size-fits-all solution to this question. A government mandate in this area would be inefficient and ineffective." – ***Rob Stoddard, National Cable & Telecommunications Association***
- "I would caution against the government deciding what defaults are the best – this is very industry and company specific (social networking vs. search, etc). Setting too restrictive default settings can result in a very negative user experience, it is better to teach users about the choices available and how to best use these choices to meet their own needs. If users (children and parents) expect certain defaults they stop being pro-active and really engaging in whether or not that default setting is the best setting for that particular use case." – ***Jill Nissen, Ning***

WHAT IS THE PROPER ROLE FOR GOVERNMENT IN THIS CONTEXT?

Holly Hawkins, AOL:

- Funding for digital media literacy and education programs targeted toward Internet safety and empowering parents and other caregivers to the online risks and tools at their disposal.

- Funding for public awareness campaigns aimed at families focusing the use of safety tools across multiple platforms (cell phones, gaming consoles, computers, etc.) in helping to protect their children.
- Funding for teacher development and curriculum in public schools addressing Internet safety.

Parry Aftab, Wired Safety

- Education, awareness, providing resources to help parents understand options, bringing the industry together, providing guidance on standards.
- Encouraging free products and the industry offering tools that work in tandem with others.
- Testing and making sure that products deliver what they promise.
- Not allowing small print, when companies offer free services and products to mine data from families and kids. Perhaps mandating standard disclosures.

Jay Opperman, Comcast

- Monitor and measure parent satisfaction with product and services and produce hard fact reports
- As a vehicle to facilitate and encourage industry improvement in products and services without mandates
- Provide funding for the education systems to develop the Digital Citizenship training programs and require Parent/Child training to grant online access privileges to under age children in schools and libraries.

Marsali Hancock, iKeepSafe

- Encourage innovation: Tax incentives for voluntary compliance to best practices.
- Provide resources and incentives for professional development for educators, parent education and curricula to be integrated into schools promoting digital citizenship and healthy online use.
- Engage the public health community to develop and implement intervention and prevention strategies for at youth risk.
- Increase resources and training for law enforcement regarding cybercrimes

Jeremy Geigle, Arizona Family Council

- Limited government regulation in the context of protecting children from the harmful effects of the internet.
- Mandated curriculum in the public schools.
- Government incentives given to technology companies (such as tax breaks or rebates) to develop and promote effective internet safety technologies.

Dane Snowden, CTIA

- Education policy and funding.
- Awareness campaigns to ensure parents are taking advantage of available tools and services and children understand how to positively use wireless devices and services.
- Help industry to identify and prioritize specific issues and strike balances between competing interests (i.e. law enforcement v. privacy advocates).

Rob Stoddard, National Cable & Telecommunications Association

- Government oversight of safety, privacy, and security is entirely appropriate.
- Government should also consider supporting and encouraging public/private partnerships to increase awareness of this issue and encourage utilization of marketplace tools. The adoption of a set of national goals for online safety and the designation of a lead agency would be very useful.
- Finally, attention to these issues by local schools, and additional research and work on curriculum development, with proper funding for both, would be helpful.

Ralph Yarro, Think Atomic

"Parents deserve the support of government in making decisions about the education of their children. The laws in place in the real world to protect children largely do not apply online, and where the law does apply, such as the prohibition on obscenity and child porn, enforcement efforts cannot keep up. The Internet is becoming increasingly essential to our children's lives. Parents, industry and the government need to vigorously continue to explore avenues to make children more safe online."

Hemanshu Nigam, MySpace

"In this context all of the pieces are already there and responsible companies have already answered the call to both make their services safer for all users and also to work with third party software providers or technologists when possible. Government would best serve its citizens by then taking the next step in the equation which is educating the public regarding the modern Internet, how their children use it, and most importantly how to engage their children on the subject of responsible Internet use."

John Morris, CDT

"Historically, government mandates in this space have been found to be unconstitutional, except in the narrow circumstance in which a government attaches conditions to discretionary funding. A mandate to require filtering, labeling, or the setting of particular defaults would certainly be overturned in the courts. On the other hand, government support for educational efforts to promote awareness of parental empowerment tools and choices would be both useful and constitutional."

Kevin Rupy, USTelecom

"Government's ideal role in this context is to raise awareness through public awareness campaigns. In addition, Government is ideally suited to support educational efforts aimed at increasing online safety. This can include efforts directed towards educating parents about digital media literacy tools, as well developing public schools curriculum on this issue."

Brian Markwalter, CEA

"[E]ven if we find that parents who are trying to use these tools are generally dissatisfied with them, one cannot conclude that government involvement will help. The companies that make a living selling these tools, online services or devices have the highest motivation to satisfy the parents paying the bills. We need to avoid asking the government to be the nanny, particularly when most parents are not asking for help."

Jill Nissen, Ning

"Government's role should be to provide funding to help educate and raise awareness."

Hedda Litwin, NAAG

"Support and fund a national public awareness campaign."

Michael Kaiser, National Cyber Security Alliance

"Education and awareness presented in a non-biased way that helps parents make informed decisions."

Braden Cox, NetChoice

"Create awareness and education. A few states—including Georgia, Louisiana, and Nevada—have passed laws that requires Internet access providers to make information available to subscribers about products or services that control a child's use of the Internet. In addition, many states now require online education into the classroom curriculum."

WHAT SORT OF ADDITIONAL STUDIES/RESEARCH WOULD BE USEFUL GOING FORWARD? WHAT QUESTIONS DESERVE MORE STUDY?

Holly Hawkins, AOL:

1. How do children of various ages use different types of technology?
2. How do parents want to monitor their child's usage of different types of technology?
3. What types of parental controls do parents use currently and what is the source of the products they use? Do these products meet their needs? If not, what is missing from the equation?

Parry Aftab, Wired Safety

1. What works and what doesn't?
2. What is in the market and what is under development?
3. What do parents want?
4. What do kids want (surprisingly, until they start liking the opposite sex, they are usually fine with parents seeing what they are doing and controlling their access (as long as the innocent sites they want are accessible)?
5. What drive parents to use, abandon or never use these tools?
6. How important is price?
7. Is one product better than several specialized ones?
8. How many households use security suites?
9. What's the current dynamic in the household on parental controls? (Older siblings setting them up, grandparents insisting on their use, etc.)

Marsali Hancock, iKeepSafe

1. New research in the US to correspond to 2009 *EU Kids Online: Final Report* (www.EUKidsOnline.net)
2. Studies around the health, safety, and well being of kids using various types of technology.
3. Studies that reflect the reach and impact and reach of IAD (Internet Addictive Disorder)
4. Studies that demonstrate the effectiveness of various approaches to Internet addiction treatments.
5. Studies to show impact of Web content on other public health concerns, particularly related to self-harm: suicide ideation, anorexia, cutting, etc.
6. Studies that demonstrate the effectiveness of education programs for prevention and intervention for primary risks youth face online (based on EUKidsOnline studies):
    - Reputation: protecting privacy/identity, giving away too much information.
    - Encountering porn
    - Encountering other harmful content (violence, hate speech, self harm information
    - Harassment/encountering unwanted sexual comments.

Hemanshu Nigam, MySpace

"As mentioned earlier there is some fantastic research in this area. In 2008 MySpace helped to form the Internet Safety Technical Task Force whose Final Report was published in December of that year. The research portion of that report demonstrated that there are many, many unanswered questions in this space worthy of research. MySpace endorses the findings of the ISTTF report and its call for future research on the following topics which could help shape policy and understanding of online child safety as a whole: minor-minor solicitation; creation of harmful content by minors; less visible groups such as LGBT youth; the interplay between socioeconomic class and risk factors; the role that pervasive digital image and video capture devices play in minor-to-minor harassment and youth production of problematic content; the intersection of different mobile and Internet-based technologies; and the online activities of registered sex offenders."

Dane Snowden, CTIA

1. *Parental Studies:* Throughout the OSTWG and other working groups, we have seen a number of studies on the ways children use digital technologies and the various affects of those technologies on children. In order to receive a more complete understanding, more research should be done on parental attitudes towards their children's technology use.
    a. What are parental attitudes toward technology? How do these attitudes affect their use of parental empowerment tools?
    b. What concerns parents about their children's technology use? What tools need to be created or modified or are available to address those concerns?
2. *Educational Studies*: How does the U.S. educational system view new technologies? How

can the U.S. educational system best utilize new technologies? (*See U.S. Department of Education, National Education Technology Plan*)

Ralph Yarro, Think Atomic

"A task force study on the effectiveness of different filter option within a controlled environment would be worth doing ("Filter Shootout"). The purpose would not be to promote one filter over another, but to gauge the effectiveness or ineffectiveness of the range of current filter solutions."

Jay Opperman, Comcast

"Long term (over months) ethnographic studies of both parent and child use of controls for younger child and communication techniques between parents and older children."

Rob Stoddard, National Cable & Telecommunications Association

1. Additional research into the effectiveness and utilization of existing parental controls tools – and on prospective features that might improve those tools – would be helpful.
2. And, since parental controls don't exist in a vacuum, research/studies on ways in which online safety controls should be combined with digital media literacy efforts for maximum benefit – in other words extending safety efforts to include "online smarts" – would be helpful.

Hedda Litwin, NAAG

1. Measuring effect of national public awareness campaign in terms of adoption of parental controls.
2. Measuring effect of standardization of controls on usage.

Jeremy Geigle, Arizona Family Council

1. The concept of internet zoning deserves to be debated in the public square and researched further.
2. Research on the mental, social, emotional and physical harms of children accessing inappropriate content.

Braden Cox, NetChoice

"I would like to see more research on how to identify and help at-risk youth. We know from various studies that it is predominantly at-risk youth that seek out inappropriate relationships with adults online, and that meet offline. How can we help these troubled youth?"

Brian Markwalter, CEA

"We should focus, or get the government to focus, on priority risks. Of the top five risks noted in the EU report [2009 *EU Kids Online: Final Report*], the first two (providing too much personal information and encountering pornography), arguably can be helped through default settings and safety tools. The others are not unique to the online world, are not conducive to technology solutions and are complicated by free speech and similar considerations."

John Morris, CDT:

"There are a broad range of potential educational and child safety programs that have been funded in the past, and a broader range of programs that could be funded in the future. With any funding, it is important that the government build in ways to test the effectiveness of the moneys given. In this and other areas of child safety (relating to, for example, drug use and sexual activity) there have been programs that sound good but later prove to be ineffective or counterproductive. We want to promote creative new ideas and approaches, but we should also seek to balance that with assessments of actual effectiveness."

Patricia Vance, ESRB

1. Parental concerns and awareness of online safety risks; what are the real "safety" issues from a parent's standpoint?
2. More nuanced information about the sorts of material/activities that parents want to block or control and how.
3. What are the different risks and preventative measures recommended for different age groups?
4. Behavioral research on *which* factors put *which* kids at risk online.
5. Consumer satisfaction with the tools available today, and why some parents don't use them.

SUBCOMMITTEE ON CHILD PORNOGRAPHY REPORTING

INTRODUCTION

This Subcommittee was charged by the Act "to review and evaluate...

> (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 under section 13032 of title 42, United States Code, including any obstacles to such reporting[.]"[53]

The Subcommittee was composed of leading experts on the issue drawn from the private sector, non-profits and academia, with input from governmental agencies. The Subcommittee strove to achieve consensus on the nature of the issues raised by the mandate and the recommendations offered by the Subcommittee. Where members felt that an issue needed further explanation, the Subcommittee provided the opportunity to the individual member to supply an addendum.

The one issue that the Subcommittee immediately encountered was the fact that the statute identified in the mandate was repealed and replaced prior to the convening of the OSTWG. In the PROTECT Our Children Act of 2008[54] – enacted three days later – Congress repealed 42 U.S.C. § 13032, the very reporting provision that OSTWG is charged with studying.[55] Title V of that Act replaced section 13032 with the more detailed service provider reporting procedure for apparent child pornography, along with other related provisions now codified in 18 U.S.C. §§ 2258A through 2258D. The subcommittee felt that it was important to evaluate the replacement statute in a manner consistent with the congressional charge. Therefore, rather than abandon the charter because of the repeal of 42 U.S.C. § 13032, the Subcommittee has undertaken to identify some of the shortcomings of § 13032, compare its reporting provisions to the superseding ones enacted as §§ 2258A and 2258B,[56] and take stock of the effectiveness of the new statute during the brief span of time since its enactment.

OVERVIEW OF SECTION 13032

Originally enacted in 1998[57] as an amendment to the Victims of Child Abuse Act of 1990, § 13032 required providers of an electronic communication service or remote computing service to the public through a facility of interstate or foreign commerce to make a report to a law enforcement agency designated by the Attorney General, as soon as reasonably possible, whenever they obtain knowledge of "facts or circumstances" indicating an apparent violation of enumerated federal statutes relating to

53 15 U.S.C. § 6554(a)(2).

54 P.L. 110-401, Title V ("Securing Adolescents from Online Exploitation"), § 501(a), 122 Stat. 4229 (October 13, 2008). The alternative short title of P.L. 110-401 is the Providing Resources, Officers, and Technology To Eradicate Cyber Threats to Our Children Act of 2008.

55 *Id.*, § 501(b)(1).

56 Section 2258C addresses the potential use of "technical elements" to stop the transmission of child pornography images of identified children – rather than addressing the reporting system itself – and § 2258D relates to limits on liability for NCMEC. Because § 13032 contained no such provisions, the Subcommittee has concluded that examination of §§ 2258C and 2258D lies beyond the scope of the OSTWG mandate.

57 P.L. 105-314, Title VI, § 604(a), 112 Stat. 2974.

child pornography.[58]

The following year, Congress amended that key reporting requirement to direct providers to make their reports, not directly to a law enforcement agency, but instead to the CyberTipline at the National Center for Missing and Exploited Children ("NCMEC"), which was charged with the duty to forward the reports to the appropriate law enforcement agency.[59] Subsequent amendments clarified the responsibilities of NCMEC, authorized it to forward CyberTipline reports to state law enforcement officials,[60] and provided limited immunity for actions taken by NCMEC in the performance of its CyberTipline responsibilities and its efforts to identify child victims.

Section 13032 was an important step forward in clarifying the roles and responsibilities of service providers as involuntary intermediaries in the channels of criminal conduct by which online child pornography is distributed. Reporting apparent child pornography under § 13032 was mandatory for providers – once they obtained knowledge of the relevant facts and circumstances – and failure to report would draw fines of up to $50,000 for an initial failure and up to $100,000 for a second or subsequent failure.[61] Appropriately, however, § 13032 also enacted limited provider immunity, assuring that actions taken in good faith by service providers to comply with the mandatory reporting requirement would not result in civil liability.[62] Perhaps most important for maintaining the proper role of providers, § 13032 made it absolutely clear that nothing in its provisions may be construed by the courts to require providers to engage in monitoring of their users, or of the content of their users' electronic communications.[63]

For all its benefits (including its brevity and simplicity), § 13032 came up short in several respects that became apparent as providers, NCMEC, law enforcement, and prosecutors gained experience with the reporting provisions.

Service providers received little guidance in § 13032 concerning just what "facts or circumstances" relating to the apparent violation of child pornography laws should be contained in the CyberTipline report. The only provision addressing the substance of the report was subsection (d), indicating that a service provider "may include additional information or material" that the provider developed (without describing what that additional information might be), except that "the Federal Government may not require the production of such information or material" in the service provider's report.[64] The vagueness of § 13032 left service providers guessing as to what additional information might be helpful or advisable to provide to law enforcement.

Needless to say, the possession and transmission of images of child pornography are federal felonies. Certainly the providers, NCMEC, law enforcement agencies, and prosecutors all contemplated that the "facts and circumstances" surrounding reportable instances might include the image of child pornography that triggered the reporting obligation. Nothing in § 13032, however, made it explicit that providers would be protected from potential criminal liability for the necessary handling and transfer of such images in the course of their mandatory reporting to NCMEC.

58 42 U.S.C. § 13032(b)(1) (1998).

59 P.L. 106-113 Appendix, enacting H.R. 3421 as introduced on November 17, 1999, § 121, 113 Stat. 1535 (codified at 42 U.S.C. § 13032(b)(1) (1999)).

60 P.L. 108-21, Title V, § 508(a), 117 Stat. 683.

61 42 U.S.C. § 13032(b)(3) (1998).

62 42 U.S.C. § 13032(c) (1998).

63 42 U.S.C. § 13032(e) (1998).

64 42 U.S.C. § 13032(d) (1998).

Law enforcement authorities also sought changes to § 13032 that would improve the reporting process and remove unwarranted impediments to investigations of child pornography crimes, such as obtaining readily accessible contact information from service providers, promoting a greater degree of standardization in the content of CyberTipline reports, and permitting NCMEC to forward CyberTipline leads to foreign law enforcement agencies.

The consensus that developed among interested parties seeking improvements in § 13032, as set forth in industry "sound practices" documents[65] and congressional testimony of both NCMEC[66] and service providers,[67] in the context of ongoing dialogue with Members of Congress and their staffs, resulted in the repeal of § 13032 and the enactment of the detailed reporting provisions of Title V of the PROTECT Our Children Act of 2008, codified as 18 U.S.C. §§ 2258A *et seq*.

SUMMARY OF MAJOR REPORTING PROVISIONS OF THE PROTECT OUR CHILDREN ACT

Section 2258A substantially expands and, in contrast to § 13032, makes explicit the range of information that service providers may include in each CyberTipline report. Subsection (a) directs providers to provide detailed contact information in the report, including an individual point of contact, while subsection (b) sets forth five categories of information that providers may include in each CyberTipline report: identifying information concerning the individual who appears to have violated a federal criminal statute relating to child pornography (such as email address, Internet Protocol address, and any self-reported identifying information); information as to when and how a subscriber uploaded, transmitted, or received apparent child pornography, or when and how it was reported to or discovered by the provider; geographic location information, such as a billing address, zip code, or Internet Protocol address; the image of apparent child pornography; and the complete communication containing the image, including data relating to its transmission and other data or files contained in or attached to the communication.

Subsection (c) directs NCMEC to forward each report to the appropriate federal law enforcement agency designated by the Attorney General, and additionally permits NCMEC to forward reports to an appropriate state law enforcement official or, if certain conditions are met, to an appropriate foreign law enforcement agency designated by the Attorney General in accordance with subsection (d). Providers must be notified by NCMEC of the disposition of reports made by the providers as the result of a request by a foreign law enforcement agency.

Subsection (e) increases the fines authorized for knowing and willful failures by providers to make the required report, up to $150,000 for a first failure and up to $300,000 for a second or subsequent failure. Subsection (f), like § 13032, prohibits the courts from construing the statute to require monitoring, either of any user or of the content of any communication of any user, and adds a prohibition against requiring providers to "affirmatively seek facts and circumstances" relating to apparent reportable violations of federal child pornography statutes. Subsection (g) tightly regulates the permissible disclosures of information contained in a CyberTipline report by law enforcement agencies (and by

65 *See, e.g., Proposed Sound Practices for Reporting Apparent Child Pornography*, United States Internet Service Provider Association, http://usispa.org/pdf/US_ISPA_sound_reporting_practices.pdf (visited March 15, 2010).

66 *See* Testimony of Ernie Allen, President & CEO, NCMEC, before the Senate Committee on Commerce, Science and Transportation, Hearing on Online Child Pornography (September 19, 2006), http://www.missingkids.com/missingkids/servlet/NewsEventServlet?LanguageCountry=en_US&PageId=2793 (visited March 15, 2010).

67 *See*, e.g., Testimony of Elizabeth Banker, Vice President, Associate General Counsel, Yahoo! Inc., before the House Committee on the Judiciary, Hearing on Sex Crimes and the Internet (October 17, 2007), http://judiciary.house.gov/hearings/pdf/Banker071017.pdf (visited March 15, 2010).

providers receiving such information to comply with legal process) or by NCMEC.

Subsection (h) contains an innovative provision intended to assure the prompt preservation of data maintained by service providers that would likely prove useful to law enforcement in investigating leads generated by CyberTipline reports. It requires providers to treat NCMEC's notification of receipt of a CyberTipline report as a request to preserve subscriber information under 18 U.S.C. § 2703(f), a well-established procedure that law enforcement routinely employs to prevent the deletion or overriding of data in a subscriber's account pending issuance of legal process to compel production of the data to investigative authorities. The new provision requires service providers to preserve the contents of the CyberTipline report and any images or files commingled or interspersed among the images of apparent child pornography within a particular electronic communication or user-created folder or directory, and to limit access to preserved data (which is likely to include material that is otherwise illegal to possess).

Section 2258B provides immunities for the entities involved in the reporting system set out in § 2258A. Section 2258B elaborates upon the immunity provision of § 13032 to bar not only civil claims but also criminal charges against service providers, domain name registrars, or their officers and employees arising from performing their duties under the new statute, unless they engaged in intentional misconduct or acted recklessly or with actual malice or for a purpose unrelated to their duty to report or preserve data. It also requires providers and registrars to minimize the number of employees who have access to images and to permanently destroy any images at the request of law enforcement.

RECOMMENDATIONS OF THE SUBCOMMITTEE

The Subcommittee notes that the reporting statute which it is our responsibility to analyze, 42 U.S.C. § 13032, by examining industry efforts to promote online safety and any obstacles to effective reporting under that statute, is no longer in effect, having been superseded in October 2008 by the provisions of 18 U.S.C. §§ 2258A *et seq.*, enacted as part of the PROTECT Our Children Act of 2008.

Having heard from a variety of experts and received presentations on a range of issues during Subcommittee meetings, it is clear that the new reporting and expedited data preservation procedures in the PROTECT Our Children Act have resolved a number of concerns expressed by providers, the law enforcement community, and NCMEC over the limitations of § 13032. In particular, two features of the new reporting and data preservation provisions of the Act were cited favorably by panelists addressing the Subcommittee.

First, as required in § 2258A(h)(3), having service providers preserve any images, data, or files commingled with the image that generated the CyberTipline report, for later disclosure to law enforcement, is likely to yield crucial evidence to investigate and prosecute offenders and successfully identify child victims. Second, having service providers forward to the CyberTipline the complete communication containing the reported image, any other images or files, and related transmission data, as called for in § 2258A(b)(5), will likely also bring to light other important investigative leads and enable the identification of child victims.

The Act appears already to have had a significant impact on the volume of CyberTipline reports made to NCMEC by service providers. NCMEC's overview of the operation of its CyberTipline, included as an Addendum to the Subcommittee report, shows that the number of CyberTipline reports received from service providers increased 84% from 2008 to 2009, the first full year the new reporting and data preservation provisions in the Act were in effect. There were 33,160 reports by providers to the

CyberTipline in 2008, and 61,055 in 2009. For the first quarter of 2010, the number of CyberTipline reports from providers totaled 27,144, on pace for another remarkable year-to-year increase of 78% from 2009 to 2010. Notably, the 2009 and 2010 CyberTipline reports include the additional images, data and other files called for in the PROTECT Our Children Act to facilitate criminal investigations of child pornography offenses and the identification of child victims. The number of images and videos reported by service providers totaled 609,206 in 2008, 700,939 in 2009, and 390,393 – for the first quarter alone – in 2010.

Overall, there has been a substantial increase in these numbers since the reporting and data preservation provisions of the Act have taken effect, which the Subcommittee hopes will accelerate investigative efforts and spur additional criminal prosecutions of child pornography offenders.

1. *Congressional commission of a survey of providers*

Regarding industry efforts to promote online safety in connection with the new reporting and data preservation regime enacted in the PROTECT Our Children Act, the Subcommittee's attempts to gather information have been only partially successful. The preferred approach to fact-finding on this issue, conducting a survey of providers of electronic communications services and remote computing services with the prior approval of the Office of Management and Budget under the Paperwork Reduction Act,[68] could not be accomplished within the time frames and resources available to the Subcommittee.

The Subcommittee recommends, therefore, that Congress task the appropriate executive agency with the objective to conduct a survey, using an empirically reliable methodology, to assess industry efforts to promote online safety by means of the new reporting provisions of § 2258A.

2. *Education and outreach to providers and law enforcement*

As noted above, the major providers of electronic communications service and remote computing service have not only been publicly supportive of the provisions of the PROTECT Our Children Act, but in fact conceived and promoted some of the original legislative proposals embodied in the Act.[69] Members of the Subcommittee expressed concern, however, that service providers at the regional and local levels, as well as some federal, state and local law enforcement agencies, may not yet be completely familiar with the new reporting provisions and data preservation procedures established in the Act. Ensuring that law enforcement officials and service providers at all levels are fully informed about all aspects of the Act will promote increased reporting, more effective investigations, and a greater number of successful prosecutions.

Subcommittee members have noted that newly established companies and smaller providers who lack in-house expertise on child online safety issues may be unaware of what to do when they encounter images of child pornography for the first time, and putting the appropriate processes in place for reporting and preservation can be daunting. Subcommittee member Parry Aftab has submitted a separate statement (included as an Addendum to this report) setting forth the challenges entailed in developing and deploying procedures to report child pornography to the CyberTipline in an efficient, safe and secure manner.

NCMEC is already helping to overcome these obstacles by engaging in extensive outreach efforts to

68 44 U.S.C. §§ 3501-3520.

69 *See* text accompanying notes 14-16, supra.

service providers to apprise them of the reporting requirements and data preservation procedures in the Act. Providers in start-up mode or those who have not availed themselves of the advice of legal counsel or other expert advisors are especially likely to benefit from NCMEC's efforts.

To cite just one example of NCMEC's outreach, service providers that submit reports manually may not be aware of significant cost savings that might be possible by automating the reporting process. To assist companies with automated reporting into the CyberTipline, NCMEC has created a document detailing the interface for its CyberTipline application to enable service providers to submit reports in "batch mode," a method of volume reporting that requires minimal human intervention.[70, 71]

The Subcommittee therefore recommends that NCMEC, government agencies, advocacy groups, and service providers continue to undertake education and information-sharing efforts to promote awareness of the PROTECT Our Children Act, particularly those provisions that widen the scope of information included in CyberTipline reports and expedite the preservation of provider data related to the transmission of images of apparent child pornography. Service providers with extensive prior reporting experience under § 2258A and its predecessor statute can assist in this effort by distributing sound practice guidelines for the benefit of providers that are just beginning to design and develop their own reporting and preservation procedures.

3. *Meetings among service providers, NCMEC, and law enforcement*

Subcommittee members who work closely with service providers emphasized that maintaining an ongoing dialogue with NCMEC and law enforcement can significantly improve providers' understanding and execution of child safety initiatives as well as performance of their reporting obligations. Too often, however, start-up companies and smaller providers fail to proactively seek out meetings with NCMEC and law enforcement, for a variety of reasons ranging from lack of acquaintance with the appropriate personnel to fear of unspecified consequences of direct engagement with law enforcement.

The Subcommittee therefore recommends that service providers, particularly those that are in the initial phase of designing processes to report apparent child pornography violations, meet with NCMEC and law enforcement agencies to broaden their practical understanding of compliance issues and help them more efficiently perform their reporting and preservation obligations under the Act.

4. *Technology and information sharing among service providers*

The Subcommittee noted the impressive collaboration that service providers and other participants in the information technology industry have undertaken for years, through joint endeavors such as NCMEC's partnership with the Internet industry consortium known as the Technology Coalition[72] and others. Through these efforts, service providers have developed and deployed innovative technological solutions that disrupt the transfer of online child pornography and facilitate reporting to

70 *National Center for Missing and Exploited Children CyberTipline II Interface* (document available from NCMEC). NCMEC has designated its service provider reporting facility as "CyberTipline II" to distinguish it from the facility for reporting by the public, "CyberTipline I."

71 As Subcommittee members noted, there may be significant up-front costs to implement automation before any cost savings can be realized.

72 See "Online Industry Leaders Announce New Effort to Use Advanced Technologies to Help Combat Child Exploitation" (publicizing formation of the Technology Coalition), NCMEC Press Release (June 27, 2006) http://www.missingkids.com/missingkids/servlet/NewsEventServlet?LanguageCountry=en_US&PageId=2442 (visited March 16, 2010).

NCMEC.[73]

The Subcommittee commends these efforts and encourages continued cooperation among industry participants. Service providers should continue their endeavors to share technologies that can support leading-edge reporting tools for use across diverse networks and platforms, in order to reduce reporting costs for all providers.

5. *Incentives to assist providers with new data preservation and security mandates*

One of the key new requirements of the PROTECT Our Children Act (described above in the summary) calls for service providers to preserve a range of images, data, and other digital files when they receive NCMEC's notification of receipt of a CyberTipline report. Subsection (h) of § 2258A instructs service providers to treat the notification as a request to preserve subscriber records under 18 U.S.C. § 2703(f), including the CyberTipline report itself (which in most cases will contain an image of apparent child pornography), together with any images, data, or other digital files commingled or interspersed among the images of apparent child pornography within a particular communication or user-created folder or directory. Gathering and segregating this data can be time-consuming and labor-intensive, particularly for providers offering high data storage capacity at low (or no) cost to users, and storing it entails additional expense for which providers have no reimbursement mechanism.

In addition, because it would be unlawful, in any other context, for private entities to store these materials, Congress imposed requirements that providers develop security measures to protect against disclosure, including maintaining the preserved files and data in a secure location, minimizing the number of employees that are provided access to images, and restricting access by agents or employees to only to what is necessary to comply with the preservation requirements. These preservation and security mandates, which are entirely appropriate and justified, nonetheless go well beyond the predecessor statute's requirement to report apparent child pornography violations. Security for ultra-sensitive data, together with access and minimization requirements, establish real infrastructure costs to be borne by providers, costs that are rapidly increasing in magnitude with the surge in the number of images of apparent child pornography reported to the CyberTipline by providers (on track to exceed 1.5 million in 2010 alone).

The Subcommittee therefore recommends that Congress consider tax credits or other financial incentives to assist service providers to bear the development and implementation costs of the preservation and security requirements established in the PROTECT Our Children Act.

6. *Incentives to establish wellness programs for compliance staff*

Finally, the Subcommittee took note of the emotional toll incurred by employees who face the task of reviewing abhorrent images of child sexual abuse in the course of their job responsibilities to fulfill their employer's compliance obligations with Congress's mandatory child pornography reporting requirements. Congress should consider providing incentives and other assistance to service providers for the specific purpose of helping establish wellness programs and other beneficial measures to address the psychological impact on employees of exposure to these disturbing images.

Separate Statements of Subcommittee Members Included as Addenda

Subcommittee member Parry Aftab of WiredSafety has provided a separate statement identifying

73 See "Microsoft and National Center for Missing & Exploited Children Push for Action to Fight Child Pornography" (announcing PhotoDNA technology to enhance detection of known images of child pornography), NCMEC Press Release (December 15, 2009) http://www.missingkids.com/missingkids/servlet/NewsEventServlet?LanguageCountry=en_US&PageId=4168 (visited March 16, 2010).

some of the costs she believes service providers incur in reporting online child pornography under the provisions of § 13032 and the successor provisions of §§ 2258A and 2258B. These costs encompass the technology, programming, and human resources necessary for (1) the initial review and reporting of images, (2) the required data preservation and storage called for in the PROTECT Our Children Act, and (3) the timely and complete compliance with legal process served by law enforcement agencies associated with reports made to the NCMEC CyberTipline. Accordingly, she expands upon the Subcommittee's recommendations relating to data preservation and security by calling upon Congress to consider additional financial incentives to help service providers put into place technologies for efficient, comprehensive, and automated reporting to NCMEC and to assist providers in hiring and retaining reporting and compliance staff. Her statement also sets forth issues for further consideration by Congress, service providers, law enforcement, and advocacy groups, including (among others) how service providers should handle "sexting,"[74] whether safe harbors based on industry sound practices would be a useful adjunct to the immunities granted under the PROTECT Our Children Act, and legal concerns arising from exposure to child pornography by providers' compliance staff.

Subcommittee member John Shehan of NCMEC provides an overview of the operation of NCMEC's CyberTipline, including statistics on reporting by members of the public as well as service providers for the period from 1998 through the first calendar quarter of 2010.

Subcommittee member John Morris of the Center for Democracy and Technology details a series of proposed factual inquiries that they believe Congress should undertake in order to evaluate how the expanded reporting system forged by the Act has affected the initiation of criminal investigations as well as the course of prosecutions in child pornography cases. Without a more complete picture of the law enforcement processes and outcomes, Congress may be hampered in its decision-making on how to allocate funding and direct oversight of the overall effort to fight child pornography.

Inclusion of Subcommittee members' separate statements provides a more comprehensive view of the concerns considered by the Subcommittee but does not represent endorsement of any additional recommedations by the Subcommittee as a whole.

CHILD PORNOGRAPHY REPORTING SUBCOMMITTEE: ADDENDUM A

STATEMENT OF JOHN MORRIS OF THE CENTER FOR DEMOCRACY AND TECHNOLOGY

Questions for Further Study

74 "Sexting" in this context refers to the creation, sharing and forwarding of sexually suggestive nude or nearly nude images by minor teenagers, usually but not exclusively on mobile devices. See Amanda Lenhart, Teens and Sexting (Pew Internet & American Life Project, 2009) http://www.pewinternet.org/Reports/2009/Teens-and-Sexting.aspx (visited April 21, 2010). Subcommittee members discussed sexting where the content includes photographs or videos that might meet the statutory definition of child pornography under 18 U.S.C. § 2256(8).

Congress directed OSTWG to evaluate the "status of industry efforts to promote online safety" through the statutorily mandated system of reporting apparent child pornography to NCMEC, and we have in this report attempted to meet that mandate. It is important to note, however, that to fully evaluate the impact of the reporting system, it is vital that Congress also evaluate the status of the investigative and prosecutorial efforts into which the reporting system flows. Without knowing how the reports are processed and handled through investigation and prosecution, it is impossible to know whether the reporting system is making a significant impact.

To illustrate this concern, the changes to the reporting system (from 47 U.S.C. § 13032 to 18 U.S.C. § 2258A) were presumably made in part to increase the level of reporting of apparent child pornography. Yet without knowing whether the investigative and prosecutorial agencies have the resources to pursue an increased number of reported cases, it is very difficult to evaluate how much impact the changes in the reporting system are actually having. And most critically, without a complete picture of the entire effort to fight child pornography, Congress cannot appropriately determine how to allocate funding or direct oversight.

To evaluate the complete picture, it would be important to collect and analyze a thorough range of data, including at least the data points listed below. A few of the data points are available, and OSTWG heard reports touching on some of the data points, but most are not available in any public form. The important data points include:

- The number of complete reports[75] of apparent child pornography received by NCMEC for relevant reporting periods (such as per month and per year), broken down by the online communications method involved (*e.g.,* websites, e-mail, etc.).
- The number of images of apparent child pornography referenced in those reports.
- The number of *unique* images referenced in those reports.
- For websites, the number of unique websites referenced, and the number of unique domains referenced.[76]
- Of reports received by NCMEC, the breakdown between emergency or expedited reports (addressing real time threats to minors) and standard reports.
- Of reports received by NCMEC, the breakdown between reports for which NCMEC determined that apparent child pornography was present, and reports where a different conclusion was reached.
- The average time NCMEC takes to process and review the expedited and standard reports, from the time received until the time a report is closed or transmitted to law enforcement.[77]
- For reports transmitted to law enforcement, a breakdown of what agencies received the reports.

75 Because of the mechanics of the online reporting system, OSTWG was told that service providers at times had to break an individual report into multiple submissions using the online system.

76 It is important that Congress receive details of the reports rather than aggregate numbers. One child pornography reporting hotline recently released preliminary information indication that out of 80,000 reports of apparent child pornography, more than 50,000 reports were duplicates (reporting the same web content, for example), and the non-duplicate reports ultimately pointed to about 600 unique websites. See Stephen Yagielowicz, "ASACP Preparing CP Reporting Hotline White Paper" (Mar. 25, 2010), available at http://www.xbiz.com/news/118917. To properly determine how best to deploy investigative funding and attention, it is vital that Congress receive and understand both the aggregate numbers (like 80,000) and the detailed numbers (such as 600).

77 To be clear, by suggesting these questions, we in no way wish to suggest a concern that NCMEC does not process the reports very promptly. Based on the evidence we heard, NCMEC appears to act with appropriate efficiency.

- For the Department of Justice and other law enforcement agencies receiving reports from NCMEC, the average time from the time of the NCMEC transmittal until (a) an initial review of the content involved was completed, and (b) formal investigative steps were undertaken.
- For the Department of Justice and other law enforcement agencies receiving reports from NCMEC, a breakdown of how many NCMEC reports (a) were pursued with an active initial investigation, (b) were not pursued because of resource constraints, (c) were not pursued because the agency did not think the content included apparent child pornography, or (d) were not pursued because of another reason.
- For the Department of Justice and other law enforcement agencies receiving reports from NCMEC, with regard to reports leading to an active initial investigation, a breakdown of how many investigations were later dropped because of resource constraints, evidentiary gaps, or other reasons, and an indication of the dispositions of the investigations that did proceed.

Only by following through to the end of the prosecutorial process can Congress fully assess the impact of the child pornography reporting system. The above facts (and certainly others that we have not identified) can provide a fuller picture of the value of the reporting system. Pursuant to Section 502(b) of the PROTECT Our Children Act, the General Accountability Office is currently conducting an evaluation of some (or all) aspects of the child pornography investigation process, with a report to Congress due four or more months after this report. We urge the GAO to consider the questions raised here in its research and report.

CHILD PORNOGRAPHY REPORTING SUBCOMMITTEE: ADDENDUM B

NATIONAL CENTER FOR MISSING & EXPLOITED CHILDREN (NCMEC): CYBERTIPLINE

18 U.S.C. § 2258A and its predecessor 42 U.S.C. § 13032 require electronic service providers (ESPs) to submit reports regarding apparent child pornography to the NCMEC CyberTipline.

Authorized by Congress and launched in March of 1998, the CyberTipline offers a means of reporting incidents of child sexual exploitation including the possession, manufacture, and/or distribution of child pornography; online enticement; child prostitution; child sex tourism; extra- familial child sexual molestation; unsolicited obscene material sent to a child; and misleading domain names, words, or digital images. The CyberTipline is staffed 24 hours a day, 7 days a week.

ESPs have submitted 44% of all CyberTipline reports received. Through the ESP reporting process, more than 6.5 million suspected child pornography image/videos have been removed from the

Internet and reported to the CyberTipline along with details of the incident.

Year	Number of Images/ Videos submitted by ESPs
1998	0
1999	0
2000	0
2001	421
2002	17,866
2003	324,166
2004	1,152,944
2005	501,587
2006	1,043,144
2007	1,830,961
2008	609,206
2009	700,939
2010*	390,393
Totals	**6,571,627**

*2010 1st Quarter only

Year	Number of CyberTipline Reports from the Public	Number of CyberTipline Reports from ESPs	Total number of CyberTipline Reports Received
1998	4,560	0	4,560
1999	9,668	0	9,668
2000	19,245	0	19,245
2001	23,482	960	24,442
2002	33,744	9,334	43,078
2003	33,857	48,102	81,959
2004	33,697	78,320	112,017
2005	39,112	31,656	70,768
2006	44,419	32,165	76,584
2007	69,414	35,847	105,261
2008	68,869	33,160	102,029
2009	58,492	61,055	119,547
2010*	17,875	27,144	45,019
Totals	**456,434**	**357,743**	**814,177**

*2010 1st Quarter only

Any incidents reported to the CyberTipline online or by telephone go through this three-step process.

- CyberTipline operators review and prioritize each lead.
- NCMEC's Exploited Children Division analyzes tips and conducts additional research.
- All information is accessible to the FBI, ICE, and the USPIS via a secure Web connection.

Information is also forwarded to the ICACs and pertinent international, state, and local authorities and, when appropriate, to the Electronic Service Provider.

NCMEC's CyberTipline is operated in partnership with the Federal Bureau of Investigation (FBI), the Department of Homeland Security's Immigration and Customs Enforcement (ICE), the U.S. Postal Inspection Service (USPIS), the Internet Crimes Against Children Task Forces (ICACs), the U.S. Secret Service (USSS), the U.S. Department of Justice's Child Exploitation and Obscenity Section (CEOS), as well as other international, state, and local law enforcement.

CHILD PORNOGRAPHY REPORTING SUBCOMMITTEE: ADDENDUM C

THE REALITIES AND OBSTACLES OF CHILD PORNOGRAPHY REPORTING FROM THE TRENCHES

By Parry Aftab, Esq., WiredSafety.org

I have practiced Internet compliance and privacy law since 1994, and have advised many industry leaders and smaller companies in child pornography reporting. Over the years, I have learned that a day-in-the-life of a service provider, social network or game network is challenging. They deal with codes, users and try to figure out the laws and best practices as best they can. Understanding their challenges will help us address child pornography reporting deficiencies better and more efficiently. This addendum is appended to the subcommittee's report (to which I contributed as a member of the OSTWG and of the subcommittee) to point out some practical implications of the child pornography reporting law. While there are ways to address and remedy these practicalities, as set forth in the entire sub-committee's report, it might be helpful to understand them from a provider's perspective.

First we should understand that providers come in all sizes, styles and levels of experience. There is no one-size-fits-all when providers are involved. Some are well-established large multi-national corporations, such as Facebook, MySpace, AOL and Microsoft. Others are either small and will stay that way, start-ups that can go in either direction or companies with new products and services that are just being developed and not well understood. Obviously the large multi-national entities have layers of risk management staff and may have someone assigned fulltime to handling child pornography and the requisite reporting and compliance issues. Others use one or more in-house lawyers or paralegals to handle these responsibilities. In some cases the head of customer service, or the company's in-house policies and abuse or moderation team is in charge of high-risk issues, including child-pornography handling and reporting. A few may assign this to their security or IT teams. And, in the case of some start-ups, even well-funded ones, they are not aware that they have a legal obligation to do anything once they discover child pornography and wouldn't know what to do even if they were aware of the law.

Notwithstanding the famous success stories of Facebook and MySpace, where start-ups quickly

become large multi-national entities and can afford trained and talented professionals to advise them on risk management, or smaller start-ups like Ning and Twitter that despite the companies' size (fewer than 200 employees) and without the same financial resources of larger companies, have devoted significant resources into legal compliance and developing best practices, the reality of being a provider these days is challenging. Personnel and IT come at a premium. Venture capitalists, banks and other common sources of funding are harder to source. Expected capital infusions no longer arrive on target. Some companies are located in out-of-the-way places and have difficulty finding local trained professionals or those willing to relocate. The competitive situation is stiff. Users of all ages are expecting online services to be provided without charge and are resisting many paid sites, networks and services. This puts further pressure on the business to cut costs and corners. While they care about doing it right and about the safety and welfare of children, they quite simply may not be able to afford to care. If it's between meeting payroll, finishing a game build or securing your data and staffing and designing a child-pornography compliance system, their continued survival might compel them to wait a bit longer to do nothing more than the bare minimum to comply with the law. As we heard from Ning, a start-up that made the decision to invest the time, money and resources not to just simply comply with the mandatory reporting requirements under §§ 2258A, but to be pioneers for a company their size in developing back-end tools that would allow them to safely, efficiently and securely provide much of the additional information that is now suggested in §§ 2258A(b) – including the actual images of apparent child pornography – doing so was extremely costly and would likely be prohibitive to many.

It's ironic that technology providers may be challenged by technology, but it's a reality. Privacy, safety and security professionals understand that products, services and systems must be designed with these risks in mind. Many large and now successful entities are still working with technologies held together "with bubble gum, chicken wire and toothpicks," as the head of IT of a social network informed me a few years ago. They are often so busy trying to manage the growth, they don't have time or the resources to manage the risks. They stick their thumbs into the dike hoping it will hold when they find new risks. They fully intend to come back and fix these problems, but often don't have the time or resources to do so, or forget that they ever existed until they arise again. Some technologies are so new that collection, storage and evidencing data is unresolved. They know they work for gaming or community interactions, but don't fully understand evidence collection and the ability to generate data reports surrounding child pornography.

And when a system is fully designed and already operating, compliance is difficult to implement. The developers and technology designers need to be informed about the compliance needs at inception. They need to understand these things *before* they code, not learn about them afterwards. Finally, who is going to pay for this and how? What are the hard and the soft costs? Do their top programmers need to be diverted from profitable builds to these "money pits"? What's the least they can get away with? There is a good deal of confusion about child pornography and what the providers are expected to do to comply. Laws change and, when they do, the whole risk management process begins anew. What had been cobbled together to comply with the previous law now needs to be re-examined by professionals to see if it must be revised or scrapped to comply with the new one. Some aren't sure they know where the "child being bathed" ends and the "child pornography" begins. Many users who report images are confused as well. While many images clearly constitute child pornography, many others fall into a legitimate grey area, or a grey area that is purely created by the provider's lack of understanding.

What about the recent rise in "sexting" where teens and preteens take, share and possess sexual images of each other? ("Sexting" combines "sex" and "texting" to reflect that a vast majority of

"sexts" are taken and transmitted using cell phones and texting devices. But sexting is not limited to handheld devices. Webcams built into most desktop gaming devices, handheld gaming devices and laptop computers, as well as those that are added to the desktop computers, are often used by teens or preteens to transmit their sexual videos to other teens or preteens (and sometimes adults). These images, although they don't fall into what had previously been thought of as "child pornography" still constitute "child pornography." MTV and the Associated Press polled teens and learned that about a third of them had sent or received a sext. They may have sent it to or received it from their boyfriend or girlfriend on a one-to-one basis, or from bullies who forward sexting images they encounter. Sometimes disgruntled ex-friends broadcast previously private images.

Questions that arise in the provider space: How does the reporting process work? And how are providers supposed to develop a faster and more efficient system for gathering the requisite information and handling the images in a legally-compliant manner? If they become aware of one image within a particular group or page, should they search through the entire group or page where the image was located to find others, even if not required to? What if they report an image and they are wrong? What if they turn over information about their users and they are wrong? What are they required to do and what is purely elective? These questions need to be answered clearly and easily if the system will be adopted across all US providers.

What are the legal implications to the provider for complying or failing to comply? It's one thing to say that there are severe penalties for non-compliance, but what about existing privacy policies that promise users that their information will not be shared with third parties other than "as may be required by court order, warrant or valid subpoena" or similarly defined law enforcement and legal compliance language? Providers may find themselves between the rock of their privacy policy and liability for violating its terms and the hard place of child pornography reporting legal compliance. Changing their privacy policy to give them the authority to turn over information "in compliance with applicable law," or "to protect the safety and security of its users, the public at large or its network" may work for prospective users and data collected following the effective date of such a revised policy, or for users who "accept" any retroactive terms by continued use or opt-in mechanisms, but won't work for anyone else. Is there a safe harbor for their complying by providing information collected under terms that prohibit its use?

What about overall risk management issues, such as human resources, security and insurance? Can they become liable for workplace safety and wellness claims resulting from emotional trauma and stress-related health issues experienced by employees responsible for reviewing the child pornography images, handling the evidence gathering or making the reports? What if their moderation teams are outsourced offshore? Should the contracts include special provisions waiving claims by the outsourced personnel responsible for this task or who may come into contact with child pornography before forwarding it on? How can they be certain that what works in the US doesn't conflict with Philippine, Canadian, Indian, Pakistani or Irish laws? Is transmitting those images across country borders illegal? If so, as many would conclude, there are additional costs involved in developing additional back-end tools and systems to allow outsourced contractors to only access that portion of the a company's servers where the child pornography is securely stored. How can they secure the images and information offshore and be confident that they have taken all necessary steps? What happens if an employee of the company misuses the images or information? What about insurance? Are there special policies they should be buying or riders they should be seeking? Do their security practices need to change? Do they have to apply encryption to the images and data they are collecting? Who legally can and who should have access to that information? How do you permanently delete illegal images once turned over or moved to special evidence storage servers?

What steps should be taken to secure the evidentiary value of the information they have on file? What works for others? Are there groups they can join to help them tackle this better? Are there financial barriers to entry to these groups for smaller companies? Are there trustworthy advisors they can afford? Is there language that they should be adopting as part of their privacy policy, terms of use or codes of conduct? If so, where can they find it? What technologies or practices have worked for others, and how much do they cost to purchase, develop or implement? Are there training programs available or professionals to help advise them? Are there watchdog groups that report non-compliers? Are there benefits, other than legal compliance itself, for complying with the law? What happens if they make a mistake and under- or over-report images?

Most industry members, large and small, established and start-up, want to comply. They care about the issues, and are often parents as well as business people. But until we can make this easier for them, and make sure their questions are answered and their confusion addressed, the laws designed to make children safer will not be as effective as they can and should be.

SUBCOMMITTEE ON DATA RETENTION

The Congressional mandate creating the Online Safety and Technology Working Group (OSTWG) called for the committee to...

> "*evaluate the practices of electronic communications service providers and remote computing service providers related to record retention in connection with crimes against children.*"

Accordingly, a subcommittee was formed to examine the practices of law enforcement, Internet Service Providers, and content and application providers concerning the retention of data that may be requested by law enforcement when investigating crimes against children. Unlike some of the other areas examined by OSTWG, there is not – either within OSTWG or the broader community – consensus on whether any data retention mandates should be imposed on service providers.

Data retention is a very contentious subject from a policy perspective. In the U.S., competing interests include those of law enforcement as they investigate crimes against children carried out or facilitated over the Internet, the Internet industry that retains certain data (primarily for business reasons), and the end-users who have privacy concerns. Consequently, this section of the report provides the three pertinent perspectives on this subject: law enforcement, industry, and consumer privacy. Ultimately, when talking about data retention we must strive to achieve the right balance between often competing and conflicting requirements.

FINDINGS

HISTORY OF DATA RETENTION

The business practice of retaining certain data related to telephone calls originated in the earliest days of telephony. Because tariffs differed region by region, or even state by state, detailed records had to be kept for each call principally so that the proper billing rate could be applied to each call and the customer billed appropriately.[78], [79] These "call detail records" contain at least the following information: the calling number, called number, the date and time of the call, call duration, and other information to facilitate bill reconciliation.

When cable system operators began to enter the telephony business in the 1990s, they began retaining data records on telephone calls made by their subscribers for similar business reasons.

Because customers sometimes disputed their bills, call detail records were kept for a few months, and then destroyed when there was no longer a business purpose for them to be retained by the service provider.

78 Since 1986 the Federal Communications Commission (FCC) has ordered the retention of telephone toll records by commercial carriers. See 47 C.F.R. §42.6. At a time when telephone service was the only real-time means of communication and when non-toll, local telephone service was largely limited to the immediate vicinity of a town or municipality, these regulations effectively require the retention for eighteen (18) months of "destination" information (i.e., "telephone number called") for every telephone call of any significant distance.

79 Not only is there an FCC requirement to retain telephony call detail records but each state has record retention requirements, principally through their state PUC. Some require that subscriber information or copies of bills be held for a handful of years.

Law enforcement and private litigants soon recognized that these call record databases contained information that could facilitate investigations and litigation. Because the telephone companies could match a telephone number in a call detail record with a subscriber's street address, both the criminal and civil justice systems began to use compulsory process to obtain these records. These records play an important part in our nation's system of criminal and civil justice because they typically represent accurate, objective, and relevant evidence generated by an otherwise disinterested third party (i.e., the provider), thereby minimizing reliance solely upon witness memory and testimony. Today, such business records continue to be used routinely by both the prosecution and defense in criminal cases, including cases involving the abuse of children.

DATA RETENTION PRACTICES TODAY

The mid-1990s saw the emergence of broad, popular use of the Internet and the "World Wide Web," as millions of users began to send email and exchange information (including still images and, recently, videos) with each other over this new communications medium. In the early days most users accessed the Internet through phone lines. Thus, phone companies could often still provide law enforcement with call detail records showing when a user dialed an Internet access number, how long they stayed connected, and what access number they dialed (but not online information such as where a user went on the Internet). For example, law enforcement could find out a subscriber dialed into his AOL account at 10 PM and stayed logged in for 2 hours by obtaining call detail records from that subscriber's phone company, but they could not determine from the telephone records what sites were visited, what messages he might have sent (or to whom), or whether he was even actually at his keyboard for the entire time he was logged in.

As more users moved to "always-on" broadband connections (using, for example, cable modem, DSL or fiber optic technology), telephone and cable telephony call detail records were of little or no use, since broadband service did not rely on telephone company switching equipment to maintain their connections. However, like their telephone predecessors, Internet Service Providers (ISPs) also need to keep track of each account in order to resolve any billing disputes, or to troubleshoot connections in the event of a failure. Once again, records kept by cable and telephone companies proved useful to law enforcement and private litigants to gather evidence for criminal or civil proceedings.

The records are generated as soon as a person connects to the Internet. Whenever a computer or home router initiates a connection over a common residential broadband access network, one of the first things that happens is that it is assigned a unique IP address by the ISP to which the household subscribes. When the user then posts a file on a website or sends an email, the IP address of the computer or home router and the date and time when those electronic communications occur may sometimes be captured. Since ISPs control only certain ranges of IP addresses, a given IP address can be traced to the ISP which assigned it. Knowing the IP address and date and time an activity occurred, the ISP can identify which subscriber was assigned that IP address at the relevant date and time. This data, which enables law enforcement to trace back from the scene of an Internet crime to find the account used to commit that crime, is part of what is often referred to as "source data," and is described more fully below.

Records from ISPs differ somewhat from telephone call records in several key aspects:

1. Internet Protocol (IP) addresses, which may identify unique computers on the Internet, are somewhat analogous to telephone numbers, but with some important differences. Phone numbers are "static," meaning the same number will usually be assigned to the

same subscriber so long as the user maintains the account. In contrast, for residential broadband connections, IP addresses are usually "dynamic," meaning that a given IP address will only be temporarily assigned to a user. A dynamic IP address is usually assigned to a user either just for a single session of Internet access, or for a brief period of days or weeks, after which, if the subscriber continues to access the Internet, the subscriber could be assigned a different IP address. Unused IP addresses are recycled back into a "pool" of addresses and can be re-assigned as needed to different subscribers. (Occasionally, however, IP addresses are "static" in that an ISP assigns one IP address to a subscriber on a long-term basis.[80])

2. An ISP generally has no knowledge of where on the Internet their subscriber has visited; all the ISP usually knows is that their subscriber was assigned a particular IP address (for example, 170.110.225.163) from time A to time B. But, unlike telephone call detail records (which are used for billing the customer), an ISP historically has had little (if any) business reason to retain information on IP address assignments.
3. IP addresses can be spoofed, i.e., someone can make their computer appear to be using an IP address that actually belongs to another user, thus making it nearly impossible to match the IP address with the right user's street address. In contrast, because telephones were generally "hard-wired" to a physical street address, spoofing of phone numbers was historically much less likely (although today, Caller-ID spoofing is possible).
4. Although possible, it is not easy for an individual to use someone else's phone service without the account holder's permission. In contrast, in cases where a broadband subscriber allows wireless Internet access without requiring a password, it can sometimes be easy for an unauthorized person to access the Internet connection. For example, someone can park nearby and connect to the Internet through a subscriber's unsecured home wireless network[81], and through that connection access any Internet content (including, possibly, illegal or pirated content).

Despite these differences, Internet records have proven to be useful to the criminal and civil justice systems.

However, there are financial and legal pressures on companies not to retain data for long periods of time. With ISPs, once a subscriber has paid their Internet access bill, there may be no incentive for an ISP to keep the record – disk storage, while relatively cheap, is still expensive when terabytes of storage are involved, over and above the costs of securing and retrieving data records from some storage archive. As for legal pressures, federal privacy and state data breach notification laws may apply to "personally identifiable information" retained by a telephony or Internet access provider, thus giving the provider an incentive to retain that information for the shortest amount of time possible or implement other affirmative measures to protect it to avoid an embarrassing and potentially costly data breach.

In addition to ISPs, operators of other electronic services, such as e-mail or interactive websites, may have data of investigative value to law enforcement. Such providers are typically referred to as "online service providers" or "OSPs." OSPs may have data sufficient to permit law enforcement to identify the user associated with a given communication (such as posting or downloading a video or sending

80 For example, a small business can purchase a static IP address from a provider so customers can always locate the company's site using the same World Wide Web uniform resource locator (URL).

81 *See* "wardriving" on http://en.wikipedia.org

an e-mail). So although the Congressional remit to this subcommittee (*supra*) uses arcane terms like "electronics communications service provider" and "remote computing service provider," this section of the report will use the more modern, Internet-era terms ISP and OSP.

ANALYSIS

The following three sections present the differing and at times inconsistent perspectives of the three major stakeholders in the data retention debate – law enforcement, Internet and online service providers, and consumer privacy advocates. These three sections were separately drafted by representatives of those stakeholder groups, and do not represent a consensus position of OSTWG.

LAW ENFORCEMENT PERSPECTIVE

Overall, industry is very supportive of law enforcement's efforts to investigate online crimes, especially crimes against children.[82] Two major difficulties, however, complicate industry's efforts to assist law enforcement. First, there exists no consensus as to what data should be retained, even across similar communication industries, and retention periods vary greatly.[83] If necessary data is no longer retained at the time law enforcement requests it, the investigation typically can go no further, regardless of how much a given ISP wants to help law enforcement. Second, although most ISPs are extremely responsive to law enforcement's requests, some ISPs lack the expertise or the resources necessary to fully assist law enforcement by providing timely, full responses to requests for information. In almost all cases, this inability to respond is not the result of an unwillingness to help law enforcement, but rather simply a lack of training or funding, especially for the smaller ISPs.

Data retention periods should be long enough to account for three significant complicating factors:

- First, child pornography collectors necessarily seek to avoid detection by law enforcement. Given the inherently secretive nature of the crime, there is often a gap in time between the commission of the offense and the discovery of the crime.
- Second, as online child exploitation investigations are sometimes international in scope, there is at times a lengthy delay before U.S. law enforcement obtains information about U.S. offenders from foreign law enforcement.[84] If the U.S. offenders' ISPs no longer retain the relevant data at the time U.S. law enforcement seeks it, those investigations dependent on Internet data will likely fail and offenders will escape liability for their crimes.[85]

82 The following discussion is conditioned by the fact that these are Internet-based crimes and crimes where relevant data is digital, as opposed to other investigations where Internet data is less central.

83 The absence of any consistent industry-wide practice to retain data for any uniform minimum duration creates uncertainty in the law enforcement community and frequently causes investigators to seek the issuance of lawful process compelling disclosure in hopes that some data may still be retained by any given provider. As discussed in the International Association of Chiefs of Police (IACP) resolution cited below, the creation of any uniform, industry-wide, minimum data retention duration practice would enable the law enforcement community to be more strategic in their requests, reserving inquiries primarily to those circumstances in which it is reasonable to believe that data would still be in existence at the time of the request.

84 Law enforcement recognizes that even if Congress were to mandate a retention period for IP address information, it would only apply to U.S.-based ISPs and OSPs.

85 As these investigations are often international in scope, it is appropriate to recognize that the European Union issued a data retention directive in 2006 generally requiring that EU member states ensure the retention of specified data for not less than six months or more than two years. See http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32006L0024:EN:HTML. It is also appropriate to recognize that some privacy advocates believe European privacy laws often better protect from disclosure to private parties the data subjected to this mandate than does U.S. law.

- Third, as online child exploitation investigations often involve an extremely large amount of data and government computer forensic resources are limited, when law enforcement seizes one offender's computer there often is a delay while that computer is examined for, among other things, leads about other offenders. Again, if those other offenders' ISPs no longer have relevant data at the time it is requested, those other offenders can go free. Particularly compelling are those investigations where law enforcement identifies a central source of child exploitation material working its way up the distribution chain from one known offender who received the material and who then re-distributed it.

The inability to identify those recipients due to the unavailability of critical provider data not only harms law enforcement's efforts, but also reinforces perceptions among child exploitation offenders of impunity and anonymity.

From a law enforcement perspective, the key challenge upon discovering an image of child pornography is determining who posted or transmitted the material. This requires linking together a string of data generated when a person goes online.

Because IP addresses are dynamically assigned (see above), it is critical to know the time zone in which the IP address of interest was located. For example, if at 3 PM a bomb threat is emailed to a school from a certain IP address in New York, and then an hour later the IP address gets dynamically reassigned to a customer in California, law enforcement could obtain inaccurate information if it queried the ISP and asked which customer had the IP address at 3 PM without specifying the time zone to which request referred, Eastern or Pacific. In the worst case, the answer would be incorrect and the police would pursue the wrong subscriber in search of their suspect.

The key to being able to link an illegal image to the person who sent or received it is the retention of the data at each stage of its transmission. First, the ISP used by the offender to access the Internet must retain the relevant data about the subscriber and the IP addresses he is assigned. Second, the OSP (such as Gmail or YouTube) that the offender used to post the video or send the e-mail must retain logs of the activity of IP addresses that have communicated with its services. If at any stage the necessary data is not retained, the investigation may come to an end and an offender could escape capture.

Therefore, in considering the creation of data retention rules, five basic issues must be addressed: (1) what data would need to be retained, (2) how long the data must be kept; (3) who would need to retain the data; (4) who would have access to the data retained, and under what conditions; and (5) what protections for consumers would be necessary.

1. What Data Would Need to Be Retained, and for How Long?

In order to complete their investigations, in general terms, law enforcement must be able to identify the subscriber or customer who was assigned a particular IP address by an ISP at a particular date, time, and time zone.

Moreover, law enforcement also must be able to identify an OSP's subscriber or customer. Like ISPs, OSPs should retain sufficient data to permit law enforcement to identify the user associated with a given communication (such as posting or downloading a file or sending an e-mail). The specific

categories of information that law enforcement may seek from OSPs parallel those sought from ISPs, but the investigative focus may be different. For example, a customer may provide inaccurate, or at least unverifiable, information when registering as a user of that OSP.[86] To provide a common example, an individual may use a false name when registering an email address with Gmail. Accordingly, the information likely to be of most investigative value includes information that the OSP user would not be able to falsify, such as records of session times and durations (i.e., when the user was logged on with that OSP) as well as IP address information.

Taken together, this data from ISPs and OSPs is referred to as "source data," that is, data that allows an investigator to trace back to the source of an electronic communication that constituted a crime on the Internet. It is this *combination* of information – both the IP address of the computer used to send the e-mail through a content or services provider and information about the ISP subscriber assigned the relevant IP address – that is critical to identifying a criminal on the Internet. If an online service provider, such as Gmail or Hotmail, does not retain connection or access data, an investigation will often be stymied at the very first step of the investigative process because law enforcement will not have enough information to take the next step of obtaining subscriber information through a subpoena to an ISP. Without the initial data point from the online service provider – often the first, crucial source of information relating to a crime – the trail of a criminal's activity on the Internet will turn cold and the investigation can end in failure.

A key variable in considering any data retention requirement is the length of time data would be retained. As noted above, current practices vary from company to company. Some retain it for less than 30 days, others for a period of months or years. Many crimes are not discovered until a significant period of time after they have been committed and, in some cases, the information critical to pursuing the case has been deleted by the time law enforcement authorities request it.[87]

2. Who Would Need to Retain the Data?

Any data retention requirement could cover three groups of companies, with slightly different requirements pertaining to each:

- First, ISPs providing Internet access to the public could be required to retain source data as described above. In fact, most ISPs already do retain source data for their own business purposes, but many do not do so consistently or for sufficiently long periods of time to be fully useful to law enforcement.
- Second, OSPs accessible by the public could be required to retain source data. Limited data retention requirements could be imposed only upon ISPs and OSPs that provide or offer a service to the general public for a commercial purpose, defined broadly. For example, it is a "commercial purpose" for a provider to offer the service free of charge to the user when the provider earns money from advertising, or when the provider obtains some other commercial benefit as a result of providing the service.
- Third, operators of "anonymous proxy" servers, whether commercial in nature or not, could be required to retain data concerning the communications they modify. Proxy servers are computers that receive, modify, and then retransmit Internet

86 Note that ISP users may also provide false names and stolen credit card information when applying for Internet service.

87 The United States Department of Justice has no official position on the issue of mandating data retention requirements. However, consistent with the October 2006 Resolution of the International Association of Chiefs of Police (IACP) which called upon all nations to enact uniform source and destination data retention requirements, the Federal Bureau of Investigation, has in the past publicly supported the retention by all public, commercial communications providers (i.e., Internet and telephony) of non-content information that would identify both the source and destination of communications for a uniform period of two years. See http://www.theiacp.org.

communications in a way that obscures the IP address used to originate the communication. That is, a proxy server assigns a user a different IP address than the one the ISP assigned to the user so that he could connect to the Internet in the first place. With that proxy IP address, the user can surf the Internet without anyone being able to trace his true identity. Those who operate proxy servers could be required to retain logs of the incoming IP addresses from their users (that is, the true IP address assigned by the ISP) and the outgoing IP addresses the proxy assigned (as well as the dates and times associated with their use) in order to permit effective investigations of offenders who use proxy servers to commit their online crimes.[88]

3. Who Would Have Access to Retained Data and Under What Conditions?

Without expressing an opinion on whether private litigants should have access to retained data, it is clear that law enforcement should have access to this data to investigate online crimes. With regard to government access to the data, it should be available on the same basis as other information on criminal suspects – that is, only through legal process such as a subpoena, search warrant, or court order.[89] This would provide an important protection for civil liberties both substantively and in terms of public perception. Furthermore, as with other legal process, a person served with process requesting retained data could be able to challenge that process in court. Such records are today covered by the Electronic Communications Privacy Act[90] (ECPA), which establishes a detailed set of rules for law enforcement access to these records.[91]

4. What Protections for Consumers Would Be Necessary?

Data retention is a controversial subject because of the perceived invasion of private information regarding individuals' Internet activity. As noted above, the requirement for legal process for access to that information protects Internet users, in large measure, from misuse by governmental authorities. However, an additional concern is the security of the retained data from misuse by third parties, either as a result of hacking or unintended disclosure. Possible solutions include: (1) the legislative creation of a federal privacy policy; (2) a prohibition on the commercial use of such data unless first rendered anonymous through an approved process; (3) a prohibition on the transfer or sale of such data; and (4) a requirement that providers have and publish a privacy policy, the violation of which would be a grounds for a breach of contract action or civil enforcement. Similarly, protection of data from hackers is also necessary. Again, various solutions are possible, including the legislative or regulatory creation of federal security standards, incentives or requirements for companies to develop security protections, or requirements that providers publish security policies, the violation of which would be a violation of their terms of service agreements.

5. Conclusions and Balancing Competing Concerns

Through the meeting of the OSTWG and otherwise, concerns have been raised by privacy advocates and members of industry about the need for mandatory data retention rules. While law enforcement respects the need for careful consideration of all issues prior to any legislation, law enforcement

88 Of course, this could have the effect of driving some proxy server operators offshore, beyond the reach of U.S. law enforcemen

89 Among the exceptions to this rule are "exigent circumstances." Under 18 U.S.C. 2702(c)(4), a provider is permitted to disclose non-content records to the government "if the provider, in good faith, believes that an emergency involving danger of death or serious physical injury to any person requires disclosure without delay of information relating to the emergency." Under exigent circumstances, the provider gains information about an emergency, either from law enforcement, a customer, or in the routine operations of its business. The provider then has the authority to disclose the information to law enforcement to prevent harm to life and limb. This disclosure is optional, not mandatory, *i.e.*, the provider can disclose the user's information if it believes an emergency situation does exist, but it does not have to disclose.

90 18 U.S.C. §2510 *et seq*.

91 See 18 U.S.C. §§2702, 2703.

respectfully disagrees that a data retention law would inappropriately invade privacy or result in the harms that others have foreseen.

For example, some privacy advocates have asserted that the benefit of data retention to law enforcement would be short term, suggesting that criminals will move their data to foreign servers. Law enforcement disagrees that this is likely to occur. While some criminals are already utilizing foreign servers to avoid U.S. law enforcement access, they are unlikely to move out of the U.S. Thus, at a minimum, data retention requirements would help to identify those committing crimes inside the U.S. For example, when foreign law enforcement seizes a server to which U.S. offenders have uploaded child pornography images that they have made – as happens routinely today – American law enforcement officers will need data stored by American providers to be able to apprehend those criminals.

Privacy advocates have also raised a concern that if a newspaper were required to collect the IP address of a user who visits its web site, it would change users' online experience. This contention appears unfounded. Today, most websites routinely capture this sort of information for marketing and technical purposes. For example, according to the New York Times' privacy policy, their website collects "tracking information collected as you navigate through [their] sites" and requires users to supply their name and unique email address to get much of their content. *See* www.nytimes.com/ref/membercenter/help/privacysummary.html.

In addition, many advocates have pointed out the positive value of current data "preservation" laws that allow law enforcement to preserve data on a limited case-by-case basis (*see* 18 U.S.C. § 2703(f), as well as the preservation rules in the PROTECT Act). While these rules are undoubtedly helpful in many situations, they unfortunately do not adequately support the investigation of child exploitation and other crimes. As numerous law enforcement witnesses at the hearing described, this system completely fails in the many situations where a crime is not promptly reported, where evidence is obtained from foreign law enforcement, and where forensic delays prevent the tracing of the offender before the data has been deleted by the provider. For example, it is extremely common to seize a computer that shows that offenders have been making and distributing child pornography for an extended period, even years, but law enforcement can only act on the very recent offenses because providers have not retained data that would allow investigators to identify earlier offenders. In sum, while preservation of evidence on a per-case basis is undoubtedly helpful – its basic form has been the law for over 10 years – it is manifestly inadequate to meet this law enforcement need. There is therefore no reason to delay implementation of data retention rules on this basis.

Moreover, some have argued that data retention would create an extraordinarily costly burden for providers. While law enforcement agrees that cost issues need to be taken into account, the cost of storage of data has dropped exponentially. Accordingly, cost issues need not preclude a focused data retention requirement, as shown by the experience of mandatory data retention in Europe.

Some advocates also suggest that retained data would create a security risk and could be intentionally or unintentionally exposed. Law enforcement understands that many companies are already collecting many types of data at issue here and are already retaining it for marketing, billing, and other reasons (albeit for shorter periods of time than needed to facilitate online investigations). While companies would, of course, need to continue to take steps to secure retained data, such steps are not so different from the ones they already take, and law enforcement is not aware of significant problems that have occurred with this type of data to date.

Further, some privacy advocates have pointed out in their arguments against mandatory data retention that the Supreme Court has recognized that the First Amendment protects the right to speak anonymously. While this general principle may be true, the cases that they point to, such as *Talley v. California*, 362 U.S. 60 (1960) and *McIntyre v. Ohio Elections Commission*, 514 U.S. 334 (1995), state general principles and do not deal with a requirement that data be retained. Instead, in those cases, the Supreme Court examined situations where a law required the speaker to disclose *to the government* his or her identity. Those cases do not reach the issue of whether the government may investigate the authorship of speech. (Indeed, in *McIntyre* the Supreme Court noted that it was not, in fact, impossible for the government to track down the author of the speech to ensure compliance with other election laws at issue.) Moreover, it is important to understand that data retention would not automatically place any information into the hands of law enforcement officials. Of course, the First Amendment would continue to protect speakers by preventing any government action to obtain that data that did not comply with the Constitution.

Finally, some privacy advocates have suggested that if Congress were to enact even a limited data retention requirement, it would be virtually inevitable that data retention requirements would be expanded to more and more classes of information, including content. This claim is apparently based on the supposition that political and other pressures would follow "notorious unsolved crimes" that could have been solved if more data had been retained. First, it does not appear that any law enforcement group has suggested that ISPs be required to retain content. More importantly, this claim is contradicted by the current situation, in which much data is retained by providers but not universally or for long enough periods. No "enormous" pressure for data retention has occurred to cause the imposition of even limited data retention requirements, let alone some unlimited version predicted by these advocates.

In sum, while law enforcement understands the need to carefully consider all sides of this issue, and to give appropriate weight to the concerns expressed by our colleagues, law enforcement respectfully disagrees that data retention sufficient to facilitate the effective investigation of online crimes would be in any way unsound, illegal, or unworkable, and believes that better data retention will allow law enforcement to solve more crimes involving the sexual exploitation of children.

SERVICE PROVIDER PERSPECTIVE

The debate over mandatory data retention has been a persistent feature of the policy landscape for years. Internet access, online service providers, wireless carriers, telecommunications and cable companies, as well as privacy advocates, have expressed unified opposition to federal and state legislative proposals that would impose sweeping data retention requirements.

Service providers fully understand the importance of digital data in investigations of crimes against children, and (as implicitly acknowledged in the law enforcement perspective, *supra*) there is a long history of cooperation and engagement between industry and law enforcement to make available critical evidentiary data promptly and comprehensively in response to valid legal process.

While opposing data retention mandates, service providers have consistently supported data preservation as a more efficient, reliable, and sensible method for making Internet and other digital records available for use in criminal investigations.

Representatives of service providers participating in the OSTWG Subcommittee on Data Retention

continue to oppose mandatory data retention requirements as overbroad, unnecessary, ineffective, and premature – particularly at this point in time (as explained below).

1. Congress should assess the effectiveness of the new data preservation requirements of the PROTECT Our Children Act before considering mandatory data retention.

In the Child Pornography Reporting section of this report, that subcommittee has summarized the data preservation requirements enacted recently by Congress in the PROTECT Our Children Act.[92] The new reporting and data preservation provisions, codified in 18 U.S.C. § 2258A, detail the information that service providers now include in their required reports of apparent child pornography crimes to NCMEC's CyberTipline – including the types of digital records that law enforcement considers critical to identifying the perpetrators of crimes against children.

This data includes identifying information concerning the individual who appears to have committed the crime (such as email address, Internet Protocol address, and any self-reported identifying information); information as to when and how a subscriber uploaded, transmitted, or received apparent child pornography, or when and how it was reported to or discovered by the provider; geographic location information, such as a billing address, zip code, or Internet Protocol address; the image of apparent child pornography; and the complete communication containing the image, including data relating to its transmission and other data or files contained in or attached to the communication.

Mandatory data retention is therefore a non-issue with respect to the data accompanying CyberTipline reports, since key information is delivered directly to NCMEC and forwarded to law enforcement even before a criminal investigation has begun.

The PROTECT Our Children Act goes a step further, however, requiring service providers to preserve for 90 days not just the CyberTipline report but also additional data that Congress determined to be important for investigating crimes against children. Subsection (h) of 18 U.S.C. § 2258A requires service providers to treat NCMEC's notification of receipt of a CyberTipline report as a request to preserve subscriber information under 18 U.S.C. § 2703(f), a well-established procedure (discussed below) that law enforcement routinely employs to prevent the deletion or overwriting of data in a subscriber's account pending issuance of legal process. The new provision requires service providers to preserve any images or files commingled or interspersed among the images of apparent child pornography within a particular electronic communication or user-created folder or directory.

The data preservation provisions of the PROTECT Our Children Act are focused and well thought-out. Congress should give this approach a chance to work, and should carefully assess its effectiveness after law enforcement has had a reasonable period of first-hand experience using the accumulated data in the investigation and prosecution of crimes against children. Only if data preservation has been shown to be ineffective should Congress consider weighing the benefits and drawbacks of the much broader and less focused scheme of mandatory data retention under discussion by this subcommittee.

2. Service providers encourage law enforcement to take advantage of the powerful tool available under ECPA.

As noted above, 18 U.S.C. § 2703(f), referenced in the PROTECT Our Children Act, already establishes a mandatory data preservation process that law enforcement has used in a wide range of digital crime investigations (not limited to crimes against children) since its enactment in 1996.

92 P.L. 110-401, Title V ("Securing Adolescents from Online Exploitation"), § 501(a), 122 Stat. 4229 (October 13, 2008). The alternative short title of P.L. 110-401 is the Providing Resources, Officers, and Technology To Eradicate Cyber Threats to Our Children Act of 2008.

The provisions of § 2703(f) are concise: upon the request of law enforcement, a service provider "shall take all necessary steps to preserve records and other evidence in its possession pending the issuance of a court order or other process," and shall retain such records for a period of 90 days, which shall be extended for another 90 days upon a renewed request by law enforcement.

Data preservation under this statutory procedure is mandatory and straightforward. Any governmental department or agency, local, state, or federal, may issue a preservation request to a service provider. No judicial action or court order is required, there is no factual showing of relevance or materiality, and no other evidentiary standard must be met.

The subcommittee heard conflicting views from law enforcement about the utility of existing data preservation authority. From the service providers' perspective the data preservation approach strikes the right balance by permitting providers to determine the optimal duration of data retention based on their business needs, while requiring them to preserve data upon request under § 2703(f).

3. Mandatory data retention will encompass vast swaths of customer data that will rarely be sought by law enforcement and prove useful in very few criminal cases, while presenting unacceptable risks to privacy and security.

Although policy discussions of data retention always generate controversy, all participants can agree on certain facts. There is no question that the vast majority of Internet users will never commit crimes, and for those who do, Internet data is likely to be irrelevant to most of those crimes. Therefore, it is indisputable that, if data retention is required by law, most of the huge mass of data collected and stored by every provider, closely tracking their customers' Internet identities, relationships, and activities, will never be useful in a criminal investigation and will never be sought by law enforcement.

Because providers would bear the costs of collecting, storing, and retrieving data for up to an estimated 230 million Internet users in the United States alone,[93] the usefulness of the infinitesimally small proportion of data that might someday be sought for a specific criminal investigation has to be weighed against the inefficiency and risks of wholesale data retention.

Internet data retention is a model that would not make sense in any other context. It is unimaginable that laws would ever require private persons to "retain" physical information such as fingerprints, left anywhere by anyone, on the chance that someday they would prove relevant to a criminal investigation. Any such law would rightly be seen as grossly out of proportion, in disadvantages and costs, to its possible value in solving crimes. When its real-world implications are examined, the value of Internet data retention envisioned by its proponents is similarly out of proportion to its disadvantages and costs.

A threshold problem in enacting mandatory data retention is how to identify, by statute, the range and type of data that providers are required to collect, store and maintain. Law enforcement in its discussion, *supra*, identifies some of the data that is currently used in criminal investigations, but Internet technology evolves rapidly and the data that is relevant today may become obsolete and irrelevant tomorrow. Legislating retention of a static set of mandatory data might limit providers' capacity to retain data generated by new products and services that might prove helpful to future investigations. Sophisticated criminals would thus have incentives to move their Internet activities to newer services that may not be encompassed in existing legislative mandates.

93 Estimate of the International Telecommunications Union for 2008, available at http://www.itu.int/ITU-D/ict/statistics/

Even assuming it could be identified in statutory language that is fortified against obsolescence by technology and evasion by criminals, the data collected by every provider must be searchable by practical means. Moreover, the results of every search must be accurate. Neither of these requirements is addressed in any rigorous way by proponents of data retention. The processing power necessary to search through exabytes of data[94] will be enormous and unprecedented, and it is not clear that every organization offering Internet access or online content in the United States will have the resources to build systems capable of undertaking such searches. Nor is it clear that accuracy can reasonably be assured when operating on databases of this expected magnitude, particularly when each provider will employ different storage and retrieval systems of varying capabilities. When human error is also factored in, mistakes may occur resulting in wrongful searches and seizures and creating potential civil liability for both providers and law enforcement officials.

Law enforcement's discussion of proxy servers *supra* is illustrative because it magnifies both of the foregoing problems inherent in wholesale data retention. Proxy servers are not offered solely to provide anonymous web surfing but are used to bring other innovative services to customers, including caching and content filtering, particularly to those millions of users who use dial-up services. Providers employing proxy servers, however, would be placed at a serious disadvantage by mandatory data retention simply because the data volumes generated by sharing IP addresses (for example) is orders of magnitude greater than assigning single, Internet-accessible IP addresses to each user. Organizations that employ proxy servers or other protocols such as network address translation – including wireless communications providers, government agencies, employers, schools, universities, libraries, hotels, airports, coffee houses, and municipalities offering public Wi-Fi hotspots – would therefore be weighed down by even greater resource demands than other providers.

Apart from its lack of practicality or usefulness in most criminal cases, amassing huge databases of personal information about nearly every American using the Internet would present new and unparalleled risks to privacy and security. The existence of disparate and widely dispersed databases encompassing our Internet identities, contacts, relationships, and communications, some of which inevitably will be poorly secured, could be fairly characterized as an "attractive nuisance" in proportion to their increasing scale and depth. The potential harm posed by unauthorized access to these troves of data is limited only by the imaginations of hackers, cybercriminals, foreign agents, and other malefactors.

Therefore, according to the law enforcement perspective, service providers would have to be subjected to a new and unprecedented regulatory regime to ensure that neither the providers themselves, nor the increasingly smarter cybercriminals, gain access to or use this voluminous data for unsanctioned purposes. Law enforcement suggests that Congress should be called upon to create overarching federal privacy policies with new prohibitions on commercial use, transfer or sale of the data, enforced against providers by breach of contract or other civil actions carrying the threat of liability for fines and damages. Similarly, law enforcement recommends congressional action to impose upon providers federal cybersecurity requirements made necessary by mandatory data retention, to be enforced in the event of violations by breach of contract or civil enforcement actions against those providers.

94 Each exabyte equals one million trillion bytes. One expert estimates that, as of March 2010, the global flow of information over wired and wireless networks totals 21 exabytes per month. Padmasree Warrior, Chief Technology Officer of Cisco Systems, speaking at the International CTIA Wireless show on March 24, 2010, quoted in Michael Miller, PC Magazine, http://www.pcmag.com/article2/0,2817,2361820,00.asp (visited May 2, 2010).

In light of its limited usefulness for criminal investigations, there is no way to justify either the risks posed by the massive accumulation of sensitive personal data, or the far-reaching extension of government regulatory power over the Internet that mandatory data retention would necessitate.

4. Summary of Service Provider Perspective

Congress should first assess the impact of the more focused and efficient data preservation procedures enacted in the PROTECT Our Children Act before considering mandatory data retention. Absent compelling reasons justifying the indiscriminate collection of data that is inherent in any broad-based data retention scheme, its drawbacks and risks far outweigh any perceived utility. Requiring service providers to retain trillions of digital records over a period of years, when none but a tiny fraction of those records will ever be relevant to any criminal investigation, will not significantly contribute to the prevention, detection, or prosecution of crimes against children. It will almost certainly create substantial risks to personal privacy and security, and give rise to regulatory and liability schemes that will weigh heavily on service providers in an already challenging economic environment, without providing tangible benefits to law enforcement in most cases.

PRIVACY PERSPECTIVE

A broad, pervasive scheme of mandated data retention by all entities in the United States that provide Internet access or that offer goods or services on the Internet would damage privacy interests and free speech on the Internet.[95] While it could benefit law enforcement in the short term, child pornographers – both distributors and users – would adjust their conduct to evade or minimize the impact of such a mandate. For example, a broad mandate could drive to offshore servers the same troublesome content now hosted in the United States; it would be accessed through offshore anonymizers not subject to the data retention requirements imposed in the U.S. A data retention mandate would also do little, ultimately, to stop the worst of the worst, and it would fundamentally change the Internet experience for people in the United States engaging in entirely lawful activity by burdening the curious and quieting the controversial. Once users understand that their Internet usage is tracked and retained, they will be less free in exploring alternative ideas available online. It would also increase the privacy impact of the inadequacies in current law which unnecessarily put privacy at risk by making more data accessible to law enforcement under low standards and inadequate process. For these reasons, the privacy community opposes mandatory data retention.

Beyond privacy and free speech concerns raised by the retention itself, data retention mandates raise serious questions about whether such retention is technically feasible and who would bear the costs of such retention. A mandate that ISPs retain IP address allocations would impose significant costs on those providers. A mandate that the other end of Internet communications – the web-based and other servers and services that citizens visit and use (provided by on-line service providers or OSPs) – retain IP addresses and other information would be an overwhelming and extraordinarily costly burden – and would certainly lead to the reduction in content and services available on the Internet. This would in turn raise serious constitutional concerns.

95 Although the Law Enforcement Perspective above disclaims intent to force all online sites to retain information, law enforcement makes clear that they want to track and monitor any website that allows users to communicate with other users. In the modern Web 2.0 world, however, that encompasses the vast majority of new and popular websites. Most new sites that offer goods and services allow users to post feedback or otherwise exchange information, and this will only increase as more sites are integrated with social networking services. Most modern sites, large and small, commercial and non-commercial, would ultimately be covered by law enforcement's proposed data retention mandates.

1. The First Principle of Data Privacy

Data retention mandates run headlong into the first principle of privacy: if the data isn't there, its privacy cannot be compromised. Currently, businesses save the data that is useful for the operation of their business, and they dispose of data that is not useful. In the case of IP address allocations, some ISPs find a longer period of retention necessary than do others. Some hold payroll data longer than do others. Some hold employee personnel records longer than do others. All of this data, and more, would be useful to law enforcement investigating some types of crime. The longer any of this data is maintained, the more at risk it is to compromise by the nefarious, or to inadvertent disclosure by the careless.

2. Preference for Targeted Data Preservation Requests

Data retention mandates would affect all users, not just the bad actors. That means that the vast majority of people whose privacy would be put at risk are innocent citizens. A far better approach – targeting the data of suspects – can be found in current law.[96] It permits law enforcement and any other governmental entity, without any judicial permission or notice at all, to require an ISP to retain data – including IP address and customer identifying information – for 90 days. The law requires no supervisory approval and no finding even within the requesting agency of specific facts that the records to be preserved are relevant to an investigation. Another 90-day period is available upon request of law enforcement. Law enforcement typically uses this power when it has identified an investigative target. In the child pornography context, current law requires that service providers *automatically* retain information whenever they make a report of possible child pornography to the National Center for Missing and Exploited Children (NCMEC).[97]

The privacy and civil liberties benefit of this approach are enormous: data about only the tiny fraction of individuals who have fallen under criminal suspicion is subject to a data preservation requirement. Everyone else would continue to enjoy the same level of privacy he or she would otherwise enjoy regardless of the law enforcement investigation. Instead of requiring ISPs and others to retain data primarily about people under no suspicion, law enforcement should focus on ways to ensure preservation of data about people who <u>are</u> under suspicion. For example, law enforcement should have additional resources – particularly in the computer forensics area – so that when a computer of a child pornography suspect is seized, it can more quickly be analyzed for leads on other offenders. This would help law enforcement quickly identify the data it needs and the entity holding the data so that a preservation order can promptly be issued. The solution to inadequate computer forensic resources should be to increase those resources, rather than to subject more data of innocent users to risk.

3. Inadequate Standards for Law Enforcement Access

Proposals to mandate data retention cannot be viewed in a legal vacuum. The privacy impact of data retention proposals must be assessed in light of the very limited privacy protections that are currently afforded to the data that would be retained. For this reason, reliance on the existing requirements

96 18 U.S.C. 2703(f), Requirement to preserve evidence, provides:

1. **In general.** – A provider of wire or electronic communication services or a remote computing service, upon request of a government entity, shall take all necessary steps to preserve records an other evidence in its possession pending the issuance of a court order o other process.
2. **Period of retention.** – Records referred to in paragraph (1) shall be retained for a period of 90 days, which shall be extended for an additional 90-day periods upon a renewed request by the governmental entity.

97 Of course, as described above in the law enforcement perspective section, the authority to preserve data does not help in cases where the crime is not immediately reported or where law enforcement uncovers data of earlier crimes.

of legal process to protect the privacy of data that would be subject to the retention mandate is misplaced.

Data retention mandates may be imposed on IP addresses and corresponding user identifying information (name, address, credit card and bank account number); this data is available with a subpoena and no notice need be made to the record subject.[98] For example, transactional data about everyone who viewed a particular web page is available with only a subpoena and without judicial oversight, even though such information (except child pornography) can be particularly sensitive. The legal process in this instance involves no proof of specific facts, no judge, and no opportunity for the record subject to object for any reason – yet reveals what content people have viewed even though they may not be targets of an investigation.

As a result, law enforcement requests for such inadequately protected data can target people who are likely entirely innocent. Were websites and other OSPs required to retain data on visitors, such information would be subject to a mere subpoena, which could, for example, be issued to require a covered provider supply identifying information about every person viewing a particular Web site. Although one could argue that this would be acceptable if the web site contained child pornography, the problem is that any data retention mandate would apply to *all* OSPs, including sites that provide sensitive, controversial, or unpopular but nevertheless lawful and constitutionally-protected content.

Take for example the person who views "jihadi websites" that glorify terrorism. Such person might be a terrorist, an opponent of terrorism, a student doing a research paper, or a person who is curious. A subpoena seeking user identifying information for every person who viewed that website – which could be followed by knock on the door or other investigative activity focused those who viewed the content – would have an obvious negative impact on free inquiry, and on free speech.

4. Extending Data Retention Mandates To On-Line Service Providers

Law enforcement has made it clear that it wants data retention mandates to reach beyond ISP access providers (which are the only entities that supply dynamic or static IP addresses) to *also* apply to OSPs. For example, YouTube is an OSP – its advertising-based sales model permits users to freely upload and view videos. Barnes and Noble is an OSP, offering for sale books and other written materials both on-line and in its brick-and-mortar stores, and invites readers to communicate with each other about the books it makes available.

Law enforcement has argued that, to be effective, a data retention mandate must apply both to ISPs and to OSPs. Otherwise, it is argued, the identifying data from the ISP cannot be linked to "crime scene" data obtained by the OSP. But a data retention mandate on an OSP news outlet like the New York Times or a video sharing service like YouTube has an enormous societal cost that must be considered. Of course, a person can post a comment on the New York Times website that consists of child pornography. But requiring the New York Times to maintain records of whenever *any* user was signed on and of the IP address used changes the on-line experience. When such a practice is disclosed to the user – as it must be – it tells the user that what he or she says is being watched and possibly saved, in a way that can be traced back by the user for later retrieval by law enforcement, all without judicial authorization and without so much as notice to the user. This would chill public discourse and encourage self-censorship at the expense of robust public debate.

98 18 U.S.C. 2703(c)(2) and 18 U.S.C. 2703(c)(3).

5. Data Retention and Anonymity

Anonymity fosters public discourse and political debate. The Federalist Papers – documents key to the founding of the United States – were published anonymously under the pseudonym "Publius," including papers authored by James Madison, John Jay and Alexander Hamilton. The James Madisons of today are no more likely to deal in child pornography than the James Madison who became President. Yet, a data retention mandate would be by definition indiscriminate and over-inclusive: it would apply to the criminal and the victim, to the politician and the dissident. Law enforcement officials use IP address and date/time stamps to associate communications with particular ISP subscribers. Because it is impossible to discern in advance the IP addresses and date/time stamps that will pertain to criminal – as opposed to lawful – conduct, a data retention mandate must cover all data.

The Supreme Court has repeatedly recognized that the First Amendment protects the right to speak anonymously. In *Talley v. California*, 362 U.S. 60 (1960), the Court said, "Anonymous pamphlets, leaflets, brochures and even books have played an important role in the progress of mankind." In *McIntyre v. Ohio Elections Commission*, 514 U.S. 334 (1995), the Supreme Court said, "Protections for anonymous speech are vital to democratic discourse. Allowing dissenters to shield their identities frees them to express critical, minority views…." Data retention mandates would diminish the possibility of engaging in anonymous speech. The very purpose of requiring ISPs and OSPs to retain IP address and date/time stamp information is to eliminate the possibility of anonymous speech, by ensuring that speech can be traced back to the person who uttered it.

6. The Steep Cliff

While some law enforcement officials have called only for mandatory retention of IP address, date/time stamps, and subscriber identifying information by ISPs to allow law enforcement to link a communication to a real person, others have made broader demands. Some seek to impose data retention requirements not only on ISPs, but on OSPs as well. Others would extend data retention mandates to more classes of data, and include even content, and have it retained for a much longer time.

It seems inevitable that once a line is crossed to mandate data retention for a limited class of data (e.g., IP address, date/time stamp, and subscriber identifying information) and a limited class of holders of that data (e.g., ISPs only), it is virtually inevitable that the data retention mandate would expand because of pressure that follows notorious unsolved crimes. If, for example, an OSP deleted records of session times, session duration, and IP address that would have identified a notorious criminal who used the OSP service for a particularly terrible crime, the pressure to require retention of such data would be enormous.

This is not just a "slippery slope" problem; it is a steep cliff problem. Once the boulder begins to fall from the top of that cliff, virtually nothing can stop it from reaching its logical resting place. In this case, the logical resting place for data retention mandates is a requirement to save content that extends not only to ISPs, but to all entities that provide services on line. In *reductio ad absurdum*, ISPs and OSPs would retain everything emanating from an end-user's computer for all time – clearly an untenable solution and lacking the requisite balance between law enforcement's legitimate needs and users' privacy rights.

7. Privacy Summary

It is clear from the discussion above that there is no current consensus on whether or how there should be mandated data retention. But there are a number of areas in which progress can be made to help law enforcement fight online crime without requiring onerous and burdensome data retention.

CONCLUSION

In the end, data retention is about striking a balance between (1) law enforcement's legitimate need to investigate and prosecute crimes against children carried out or facilitated by the Internet; (2) end-users' legitimate privacy expectations and the democratic ideals of anonymous and free speech; and (3) ISP/OSP costs of retention, costs that ultimately get passed onto consumers and, if these costs were to become onerous, could have the effect of stifling innovation and creativity on the Internet. Today, there is no clear consensus, as the foregoing sections have demonstrated, on how best to improve that balance. Here are some steps that could be considered:

- The ICAC task forces (there are 61 spread across the U.S.) hold regular meetings. ISPs and OSPs should have similar meetings, and joint meetings between the two groups, as well as federal law enforcement agencies, could take place quarterly or semi-annually. These meetings would be a means for industry and law enforcement to share information about emerging threats, resolve operational glitches, and develop new practices and procedures, if necessary.
- Consumers have their privacy expectations, and vast amounts of stored data raise significant privacy concerns.
- The data retention debate, if there is to be one, should take place at the federal level. As the foregoing perspective sections indicate, there is no consensus among the three major stakeholders on what data retention rules should be. If states are allowed to set their own data retention standards, this would burden the ISPs/OSPs with as many as 54 different sets of requirements, creating even more uncertainty for law enforcement.
- Congress should first assess the impact of the more focused and efficient data preservation procedures enacted in the PROTECT Our Children Act before considering mandatory data retention.

In summary, assessing the necessary balance between the retention needs of law enforcement, the requirements of ISPs/OSPs, and the privacy interests of consumers is a complex area. The subcommittee recommends that Congress carefully consider these often competing concerns before considering data retention rules.

APPENDIX A

The Online Safety and Technology Working Group wishes to thank the following people for generously giving of their time to assist us in our work:

Ellen Agress
Joe Alhadeff
Nathan Andersen
Carolyn Atwell-Davis
Traci Beagley
Jacqueline Beauchere
Cliff Boro
Bonnie Bracey
David Burt
Karen Cator
Ann Cavoukian
Michelle Collins
Chad Coons, Jr.
Chuck Cosson
Kate Dean
Norris Dickard
Leslie Dunlap
Kelli Emerick
Don Eyer
David Finnegan
Jorge Flores
Dona Fraser
Jill Geigle
Matt Gerst
Emily Hancock
Pamela Jones Harbour
Mary Heston
Julie Inman-Grant
Jasmine Johnson
Rick Lane
Jennifer Leach
Sally Linford
Emma Llanso
John Logalbo
Cynthia Logan
Roarke Lynch
Edwinna Lyuck
Carol Magid
Phyllis Marcus
Allan McCullough
Tim McShane
Eliot Mizrachi
Greg Nojeim
Lindsey Olson
Julia Plonowski
Cheryl Preston
Jason Rzepka
Kim Scanlan
Kim Scardino
Kristen Schoenenberger
Jamie Marie Schumacher
Stephen Sharon
Allan Smart
Rick Smith
Chris Stetkiewicz
Margaret Sullivan
Catherine Davis Teitelbaum
Frank Torres
Chris White
Art Wolinsky
Lori Wood

APPENDIX B

AGENDAS OF OSTWG MEETINGS

JUNE 4, 2009

Introductory Meeting

Location: Federal Communications Commission Meeting Room
445 12th St. SW, Washington, DC 20554

Time: 10 am to 2 pm

AGENDA

10:00-10:10 Call to Order and Welcoming Remarks by OSTWG Co-Chairs Anne Collier and Hemanshu Nigam

10:10-10:20 Opening Remarks by Anna M. Gomez, Acting Assistant Secretary of Commerce for Communications and Information

10:20-10:35 Remarks by Susan Crawford, Special Assistant to the President on Science Technology & Innovation

10:35-11:00 Video Presentation of Recorded Talk by KSU Professor Michael Wesch, given at the Library of Congress

11:00-11:30 Introductions by Working Group Members (going "around the table")

11:30 to 11:45 Break

11:45-12:30 Remarks by Federal Government representatives (FCC, FTC, DOJ, and Education) on government role and online safety work to date

12:30-1:30 Remarks by Subcommittee Chairs
a) Education Subcommittee (Larry Magid)
b) Data Retention Subcommittee (Michael McKeehan)
c) Child Pornography Reporting Subcommittee (Chris Bubb)
d) Protection Technology Subcommittee (Adam Thierer)

1:30-2:00 Closing Discussion

2:00 Adjournment

SEPTEMBER 24, 2009

Meeting on Internet Safety Education

Location: U.S. Department of Commerce Room 4830
1401 Constitution Ave. NW, Washington, DC

Time: 9 am to 4:30 pm

AGENDA

9:00-9:30 Welcome and Opening Remarks by OSTWG Co-Chairs Anne Collier and Hemu Nigam and Assistant Secretary of Commerce Larry E. Strickling

9:30-9:35 Introduction by Subcommittee Chair Larry Magid

9:35-10:20 Student Panel – D.C. public school students

10:20-10:30 Break

10:30-11:00 How Industry Educates, Stephen Balkam, Family Online Safety Institute

11:00-11:30 How Schools Educate, Nancy Willard, Center for Safe and Responsible Internet Use

11:30-12:00 Cyberbullying – local case study, Mike Donlin, Seattle Public Schools

12:00 Lunch Break

12:30-12:35 Welcome and Introductions, Danny Weitzner, Associate Administrator, NTIA Office of Policy Analysis and Development

12:35-1:05 Jessica Gonzalez, consultant to National Hispanic Media Coalition, on Hate Crime

1:05-2:00 How NGOs Educate (OSTWG members plus special NGO guests)

2:00-2:30 Risk Prevention Education in the Online Environment – Patti Agatston, PhD, Cobb County (GA) Schools

2:30-3:00 Digital Citizenship & Media Literacy Education, Alan Simpson, Common Sense Media

3:00-3:45 How Youth are Using Social Media, Prof. Henry Jenkins, Ph.D., University of Southern California

3:45-4:30 General Discussion

4:30 Adjournment

NOVEMBER 3, 2009

Meeting on Parental Controls, Child Protection Technologies, and Content Rating Methods

Location: U.S. Department of Commerce Room 4830
1401 Constitution Ave. NW, Washington, DC

Time: 8:30 am to 5 pm

AGENDA

8:30-8:45 Welcoming Remarks, Lawrence E. Strickling, Assistant Secretary of Commerce for Communications and Information

8:45-9:00 Opening remarks from Rep. Debbie Wasserman Schultz

9:00-11:15 Panel 1: Network-based & Independent-Provided Online Safety Tools

Moderator: Adam Thierer
Discussants: Karen Hullenbaugh, Director of Safety Products, AOL; Dane Snowden, Vice President, External and State Affairs, CTIA–The Wireless Association; Forrest Collier, Chairman & CEO InternetSafety.com/Safe Eyes; Rob Stoddard, Senior VP, Communications & Public Affairs, National Cable & Telecommunications Association; James Dirksen, Managing Director, RuleSpace; Marian Merritt, Internet Safety Advocate, Symantec; Cheryl Preston, Brigham Young University Law School and Think Atomic; Kevin Rupy, Director of Policy Development, USTelecom

11:15-11:30 Break

11:30-12:00 Panel 2: OS-level, Browser-based & Search-Oriented Tools & Methods

Moderator: Adam Thierer
Discussants: Frank Torres, Director of Consumer Affairs, Microsoft; Scott Rubin, Global Communications & Public Affairs, Google; Emily Hancock, Senior Legal Director, Yahoo!

12:00-12:30 Lunch Break

12:30-1:00 Luncheon Remarks from Will Gardner, CEO, Childnet International in London and Dr. Hoda Baraka, First Deputy, Egyptian Minister of Communications and Information Technology

1:00-2:30 Panel 3: Social Networking and Web 2.0 Approaches to Online Safety

Moderator: Tim Lordan
Discussants: Phyllis Marcus, Senior Staff Attorney, Federal Trade Commission; Jill Nissen, Vice President, Chief Policy Officer, Ning; Susan Fox, VP, Government Relations, Walt Disney Company/Club Penguin; Reggie Davis, General Counsel, Zynga

2:30-2:45 Break

2:45-4:00 Panel 4: Other Perspectives on Tools, Ratings & Online Child Protection

Moderator: Tim Lordan
Discussants: Todd Haiken, Senior Manager of Policy, Common Sense Media; Pat Vance, President, Entertainment Software Rating Board; Kim Mathews, Attorney Advisor, Media Bureau, Policy Division, Federal Communications Commission; Orit Michiel, Vice President and Domestic Counsel, Motion Picture Association of America; Stuart Rosove, Vice President for Media & Entertainment, Digimarc

4:00-4:30 "Digital Ethics Among Digital Youth," a talk by Carrie James, PhD, of the Harvard School of Education's GoodPlay Project

4:30-5:00 General Discussion

5:00 Adjournment

FEBRUARY 4, 2009

Meeting of the Child Pornography Reporting and Data Retention Subcommittees

Location: U.S. Department of Commerce Room 4830
1401 Constitution Ave. NW, Washington, DC

Time: 8:40 am to 5 pm

AGENDA

8:40-9:00 Opening remarks from Co-Chairs Anne Collier, Hemanshu Nigam, and Deputy Assistant Secretary of Commerce Anna Gomez

9:00-9:05 Opening remarks from Subcommittee Chair Chris Bubb

9:05-9:30 "Social Media Trends," Amanda Lenhart, Pew Internet and American Life Center

9:30-10:00 "CP Reporting 101," John Shehan, NCMEC

10:00-11:10 Law Enforcement Panel and Discussion

Bob O'Leary (Moderator); Drew Oosterbaan, Chief, CEOS, Department of Justice; Nicholas Savage, FBI SSA; Gerard F. Meyers, SAIC Iowa Internet Crimes Against Children Taskforce

11:10-11:20 Break

11:20-12:30 Industry Panel and Discussion

Kate Dean, USISPA (moderator); Chris Bubb, AO; Elizabeth Banker, Yahoo!; Frank Torres, Microsoft; Jill Nissen, Ning; Brooke Batton, United Online; Michael Sussman, Perkins Coie

12:30-1:15 Lunch Break

1:15-1:20 Opening Remarks from Data Retention Subcommittee Chair Mike McKeehan

1:20-1:45 "What, Exactly, Do we Mean by Data Retention?" Drew Arena, Verizon

1:45-3:05 Law Enforcement Panel And Discussion

Paul Almanza, Department of Justice (Moderator); Matt Dunn, Department of Homeland Security/ICE; Dr. Frank Kardasz, AZ ICAC; Gerard Meyers, Iowa ICAC; Gregg Motta, FBI

3:05-3:15 Break

3:15-4:25 Panel and Discussion: "Data Retention in Practice: Industry and Privacy/Civil Liberties Perspective"

Declan McCullagh, CNET (Moderator); Kate Dean, USISPA; John Morris, Center for Democracy & Technology; Chris Calabrese, ACLU; Dave McClure, USIIA; John Sevier, Davis Wright Tremaine

4:25-5:00 General Discussion

5:00 Adjournment

MAY 19, 2009

Final OSTWG Meeting

Location: U.S. Department of Commerce Room 4830
1401 Constitution Ave. NW, Washington, DC

Time: 1:30 pm to 5 pm

AGENDA

1:30-4:00 Opening Remarks from Hemanshu Nigam and Anne Collier, OSTWG Co-Chairs, and Lawrence E. Strickling, Assistant Secretary of Commerce for Communications and Information

1:40-3:00 Review and Refine Subcommittee Recommendations and Report Language

3:00-3:10 Opening for Public Comment

3:10-3:25 Break

3:25-4:45 Continuation of Report Review

4:45-5:00 Opening for Public Comment

5:00 Adjournment

APPENDIX C

STATEMENTS OF OSTWG MEMBERS

Parry Aftab (WiredSafety) Statement - OSTWG Report (full version aftab.com/ostwg)
It has been an honor to serve on the OSTWG, a varied and stellar group. Each brings something special to the table. Because WiredSafety and my experience, especially our work with victims, parents and young people, differs from that of many working group members[1], while we concur with most of the conclusions reached in the Report, we differ on several others.

The most significant differences relate to the importance of law enforcement and the scope and prevalence of cyberbullying (where one minor uses digital technologies as a weapon to hurt another minor), sexting (taking, sending or possessing nude or sexual images of minors by minors, including of themselves) and sexual exploitation of minors by adults that is facilitated by digital technology. Based upon our 15 years in the field, we believe that more minors are victimized, victimizing each other and putting themselves at risk than the Report reflects. Things that are obvious face-to-face are less obvious online. While we agree that the education of young people about safe and responsible digital technology use is critical, under the right set of circumstances even a well-educated child could become an unwitting victim. It is the role of our police to keep this from happening. That is why we shouldn't lose track of the importance of well-trained and equipped law enforcement agencies and their role in our children's safety online and off.

At the same time, we recognize that the public (and parents, in particular) often over-estimate the risks children face online, especially when sexual predators are involved. (We fear what we don't understand, which is why parental education is so important.) While we have to correct their misconceptions, under-estimating the risks is not the answer. In our opinion, the Report leaves the impression that our young people are less at risk than our experience leads us to believe. How serious are the risks? Sadly, we can only guess. When it comes to cyberbullying, sexting and sexual exploitation of minors facilitated by digital technologies, we don't really understand the facts. We don't know how often they occur, to whom they occur and the seriousness of the victimization/harm. Why? Because our children often don't understand that they have been victimized, intentionally hide the victimization from us or don't share the truth when asked by researchers conducting academic surveys. (Only 5% of students polled told us that they would tell their parents if cyberbullied.) While under-reporting is an offline reality, it is worse when young people feel they have been complicit in some part of the digital abuse.

We are among the experts who believe that cyberbullying is at epidemic levels especially in middle school, and that more minors and at increasingly younger ages are engaged in taking, sending or receiving nude or sexual images. (Our survey of children 10 -12 disclosed that 5% had sent a sexually provocative, nude or sexual image and 6% had received one. Teenangels.org/sexting.) The MTV/AP survey conducted for the digital abuse prevention campaign, athinline.org (for which one of my Teenangels and I are advisory board members), shows a higher incidence of sexting than reflected in the Report, as well. This is particularly concerning, as those admitting to sending a sext also admitted to being more than 3 times more likely to consider suicide. The more we know, the better job we will be able to do. For that we have to engage young people, ask the right questions and demand better answers.

---

[1] WiredSafety served on the Harvard Berkman Center's ISTTF. It and I bring knowledge of cybercrime, law, privacy, best practices, victim-assistance, youth leadership and peer-education, parent education, mommy blogging and issues involving cyberbullying and the digital technology social and sexual conduct of minors. (To learn more visit WiredSafety.org.)

U.S. Department of Justice Addendum to the OSTWG Report

The U.S. Department of Justice ("Department") was pleased to contribute to the OSWTG process. This Addendum, concerning one issue, should not be interpreted to mean that the Department necessarily endorses the remainder of the OSTWG Report.

By stating that "several studies, including some funded by the U.S. Department of Justice, have shown that the statistical probability of a young person being physically harmed by an adult who they first met online is extremely low," the Report's Education Section could be read to indicate that the risk that online sexual predators pose to children is very small.[1] The research by the Crimes against Children Research Center ("CCRC") of the University of New Hampshire discussed in this portion of the Report was based in part on telephone interviews with youth ages 10-17 whose parents or guardians were notified that the interview would discuss "sexual material your child may have seen" and who then gave permission for such interviews. Although the interviewers told the youth their responses would be "confidential," readers should recognize that it is at least possible the pre-teenage and teenage youth who were interviewed, knowing that their parents were aware they were being questioned about their online activity involving sexual material, may have distrusted the confidentiality of the survey and underreported that activity for fear that their parents would learn that they had engaged in certain behavior or practices online of which their parents would disapprove.[2]

The Department disagrees with any implication that the risk online predators pose to children is extremely small. For example, reports of online enticement of children for sexual acts to the National Center for Missing & Exploited Children's CyberTipline increased from 707 in 1998 to 5,759 in 2009. Moreover, documented online enticement complaints processed by ICAC Task Forces, which include both complaints based on undercover operations where agents pose as minors and complaints based on the enticement of actual minors, increased from 3,572 in 2004 to 8,313 in 2008. The information presented in the Education Section should thus be considered in context, given this data.

Because the health and safety of our children is important to us as a society, we devote significant resources to combating these serious crimes through education, by investigating and prosecuting the offenders, and by providing services and restitution to crime victims. These resources are well spent because providing education and training to better protect children and to assist law enforcement in identifying perpetrators, rescuing child victims, and training law enforcement and court personnel to handle these cases more effectively is a critical component in our strategy to prevent child exploitation. Accordingly, while the Department agrees that research will assist in targeting sound prevention messages to the populations those messages will most benefit, and that prevention messages should include teaching social responsibility as a core component of personal safety, the Department believes it important that prevention messages not minimize the risk to children posed by online predators.

The Department will soon be releasing a Report to Congress on The National Strategy for Child Exploitation Prevention and Interdiction ("National Strategy"), as required by the PROTECT Our Children Act of 2008. The Department invites readers to review the National Strategy, which will include a detailed assessment of child exploitation threats, including an assessment of the threat of online enticement.

---

[1] Of course, points of view or opinions stated in Department-funded research are those of the authors of the research and do not necessarily represent the official position or policies of the Department.

[2] The first CCRC youth telephone survey was conducted between 1999 and 2000, and the second in 2005. Given the rapidly-changing nature of the Internet, readers may wish to consider the age of this research.

Statement of Anne Collier
Co-Chair
Online Safety and Technology Working Group
Co-Director
ConnectSafely.org **June 4, 2010**

As Hemu and I stated in the Executive Summary to this report, we are indebted to the insightful, collaborative work of our fellow OSTWG members, especially that of our remarkable subcommittee chairs, Chris Bubb, Larry Magid, Mike McKeehan, and Adam Thierer. We can't thank them enough. And I can't thank my co-chair, Hemanshu Nigam, enough for all the experience and hard work he brought to our task.

We are also grateful for the dedicated support of the National Telecommunications and Information Administration. NTIA staff did a lot more than gather and advise the Working Group, and we are thankful to them for many hours of support often well beyond "business hours."

The statute that called for our formation did not ask us to advance the public discussion about youth online safety, but we felt it imperative to do so. In addition to the challenge of responding fully to the statute, we were challenged with the task of building on the fine work of the COPA Commission, the Committee to Study Tools and Strategies for Protecting Kids from Pornography at the National Research Council, the Internet Safety Technical Task Force at Harvard University's Berkman Center, and many other blue-ribbon bodies in the US and other parts of the world.

With the insights from social media scholars, educators, and risk-prevention practitioners represented in this report, I am delighted to say the OSTWG Report does indeed advance the discussion. Our report puts on record the latest thinking on youth online safety, from risk-prevention practitioners' call for application of the public health field's three-tiered prevention model to recognition of the need for a coordinated, multi-disciplinary approach to youth online safety at the federal level.

It's now time to move forward, with targeted, evaluated online risk prevention and intervention by all fields working in child protection; coordinated, multidisciplinary federal government support; a national commitment to pre-K-through-12 instruction in digital media literacy and citizenship; and...

...as we say at ConnectSafety.org, Internet safety set in the positive context of young people's full, constructive engagement in participatory media, culture, and democracy.[i]

---

[i] "Online Safety 3.0: Empowering and Protecting Youth" (http://os3.connectsafely.org)

Promoting Convenience, Choice, and Commerce on the Net

The NetChoice Coalition
1401 K St NW, Suite 502
Washington, DC 20005
202.420.7482

www.netchoice.org

NetChoice Comments on Final Report of the Online Safety and Technology Working Group

NetChoice is thankful to have participated on the Online Safety and Technology Working Group (OSTWG). During the past year, we have heard from experts on a number of various issues related to child safety on the Internet. This report reflects the thoughtful insights of these experts and the hard work of OSTWG members.

Importantly, the report is the most up-to-date snapshot of the online safety efforts of educators, industry and law enforcement. Overall, it is overwhelmingly positive great strides have been made in understanding the nature of the threat and how to respond:

- Most youth capably deal with Internet problems. Parenting styles are strongly related to online experiences, behaviors and attitudes.
- Harm prevention needs to be tailored to risk, and online risk correlates with offline risk.
- The parental controls technology marketplace continues to evolve rapidly and work best in tandem with educational strategies, parental involvement, and mentoring.

Understanding the true risks of online communications is the first step toward crafting public policy solutions. In this regard, there are important recommendations for policymakers:

- Government should avoid inflexible, top-down technological mandates.
- Media literacy should be a national priority.
- Congress should assess the effectiveness of current data preservation requirements before considering data retention mandates.

The report underscores the privacy and free speech interests of citizens when using Internet communications, and the tensions that exist with law enforcement desire to access data. NetChoice believes that the Electronic Communications Privacy Act (ECPA) should be amended to reflect modern Internet communications. Updating ECPA would go a long way to allow online computer services to better provide and preserve data for law enforcement investigations, while still protecting the constitutional rights of citizens.

But perhaps it is what the report does not include that is of equal importance to Congress and other policymakers. OSTWG specifically considered and rejected a recommendation for online content and service providers to develop parental control technologies according to a common language. The working group recognized the risk that standardization could freeze innovation and make it more difficult for online services to create user interfaces tailored to their products.

Going forward, NetChoice will continue to work with state, federal and international policymakers to implement the report recommendations and further improve online safety for children.

Online Safety Technical Working Group
Brian Cute
Comments

Online safety is a complex, dynamic and fluid challenge for youth, parents, industry, society and the government. My participation on the Online Safety Technical Working Group (OSTWG) has served to confirm this fact. The dynamic nature of the Internet presents something of a moving target when trying to identify the surest, most predictable ways to disseminate useful information concerning safe Internet practices to youth and adults alike. The interaction of all stakeholders is critical and yet no single stakeholder can deliver the silver bullet solution to this challenge. What remains constant is that the school system provides an environment in which online safety practices can be communicated to the youth of America in a structured and meaningful way.

What became painfully obvious in our exploration of online safety in the school setting is that the introduction of Internet safety training through the traditional channels of "curriculum development" and "teacher training" will take too long to equip today's youth with the necessary tools to use the Internet as responsible Digital Citizens. Indeed it will be years before we can answer such questions as "should Internet safety be its own subject matter" or "should Internet safety be developed as adjunct curriculum to computer and IT studies" or "should Internet safety be integrated across all existing curriculum as a 'cross cutting' issue." All the while, our children will be adopting the latest Internet or gaming technologies, blithely exposing themselves to new risks or inadvertently allowing malicious actors to perpetuate nefarious practices through young users' ignorance of basic computer and Internet "hygiene."

The OSTWG Education Subcommittee's recommendation to "Create a Digital Literacy Corps for Schools and Communities Nationwide" should be our most pressing national priority. Finding creative means to get instruction on Internet safety into the school setting today is critical. Programs like AmeriCorps or modifications to existing student grant or loan programs could attract capable college aged students or graduates to deliver Internet safety study into the school setting in the short term. This first wave of Internet safety instruction should be set in motion while structured curriculum development and teacher training processes proceed in parallel. The creation of a Digital Literacy Corps is the first critical step down this all important road.

ARIZONA FAMILY COUNCIL

Prior to the Internet, great efforts were made to protect children from inadvertent and intentional exposure to pornography. Today solid, concrete barriers exist in the physical world such as criminal laws, zoning laws, restrictions on retail establishments, identification verification, etc. to help prevent children from being exposed to pornography. The virtual world, however, provides breakable and in many instances, non-existent barriers to even inadvertent exposure to pornography.

The harm from exposure to pornography is a significant risk children face on the Internet today. It is no longer a question of *if* a child will be exposed to pornography, but *when*. 9 out of 10 children ages 8-16 have viewed Internet pornography, usually unintentionally (London School of Economics, January 2002). A study from Columbia University reports that 75% of boys ages 16-17 *regularly* view and download pornography. Not only is pornography reaching most of the Internet child population, it is having a negative effect. The minimum harm to children from exposure to pornography is poor sex-education and degrading views of women. Some of the more severe harms are sexual crime and addiction. A study of juvenile sex offenders reports that twenty-nine out of thirty offenders had viewed x-rated materials at an average age of seven and a half.

Because children can be severely harmed by exposure to pornographic materials, more needs to be done to:

- educate teachers, parents and children of the potential harms - Internet safety education needs to include information on the addictive nature of pornography;
- build upon the research of the mental, physical, social, emotional, familial and relationship harms of pornography exposure - Responsible government should fund more medical and scientific research on the harms to children from exposure to pornography;
- establish solid, concrete barriers in the virtual world to protect children from these harms through legislative, law enforcement and free-market incentives – families need to be empowered with options to protect their children on the Internet.

Children's exposure to pornography online is just as damaging and threatening as any other online threat because it grooms victims and perpetrators of sexual crimes, introduces children to an illegal and addictive substance, and robs them of an age of innocence worth protecting. Because of the latest medical and scientific research, pornography is not solely a moral issue. It is a public health and societal issue. More needs to be done by government and society to protect children, families, and our communities from the harms of children being exposed to pornography.

Resources:
Media in the lives of 8-18 year-olds http://www.kff.org/entmedia/8010.cfm
"The Social Costs of Pornography" by the Witherspoon Institute
http://www.internetsafety101.org/upload/file/Social%20Costs%20of%20Pornography%20Report.pdf
"The Harms of Pornography Exposure Among Children and Young People" by Michael Flood
http://www.xyonline.net/sites/default/files/Flood,%20The%20harms%20of%20pornography%20exposure%2009.pdf

OSTWG Report: Appendix D
iKeepSafe Statement

iKeepsafe would like to thank the OSTWG committee members for their thoughtful contributions to the final report. We anticipate that this effort will help congress as it allocates resources, sets policy, and encourages industry regarding child safety and privacy online.

We encourage all stakeholders (industry, policy leaders, public health, education, law enforcement, parents and youth) to consider how all aspects of an incident might be better handled:

- ***Pre-Incident:*** Prepare for an incident by developing easy-to-use reporting mechanisms that interface with public health and law enforcement. Develop policy, implement prevention/intervention programs, and establish protocol for incident management.
- ***At the time of Incident:*** Implement strategies on how best to respond to the victim, perpetrator, and any bystanders of an incident (i.e., fact finding, documentation, and reporting when necessary).
- ***Post-incident assessment:*** Follow-up with the parties involved. Track outcomes of response, trends, and implement redesign of reporting mechanisms where helpful.

Pre-incident
Industry can provide more robust family and privacy settings across all platforms, with streamlined connectivity management for parents and reporting mechanisms. We recognize that many providers of Web and mobile products have made noticeable strides to simplify and streamline family settings and reporting mechanisms whereby users and their parents can report inappropriate content, bad behavior/harassment, and terms of service violations. Despite these efforts, most parents remain overwhelmed by the requirements of managing family and privacy settings. Going forward, we encourage industry to voluntarily come together to streamline (where possible) family settings across platforms, so that once a parent has mastered the controls in one platform, he or she can transfer that expertise to other venues. We recognize the need for businesses to differentiate their products and protect their brands, and we are confident that individuation can be maintained while still improving usability and uptake of online safety features in homes. We also encourage industry to offer products with the family settings enabled as default.

At the Time of the Incident
Industry can reach out to bystanders by providing robust ways for them to self-police their communities and to intervene when they see a peer engaging in high-risk/illegal online behavior or harassment (either as victim or perpetrator). Bystanders should be able to quickly respond by reaching public health venues through online mechanisms when they see evidence of suicide or other life threatening situations.

Post-incident
One area where congress can make a significant difference is in providing funding for research and professional development to law enforcement, education and public health communities. We see very little funding to help public health and education communities be more effective and relevant as they respond to youth needs in a digital environment and preparing youth for full digital citizenship.

We are hopeful that as the technologies surrounding connectivity improve, the safety and privacy management features will grow with them towards a more friendly, plug-and-play interface where non-technical users find safety features and content filtering enabled as the default and where problems can be resolved through easy, established channels.

Marsali Hancock, President
Internet Keep Safe Coalition

The National Cyber Security Alliance (NCSA) is **not** submitting a dissenting point of view about this report.

NCSA joined OSTWG assuming that to be a success the final report to Congress would be inclusive of a broad range of viewpoints and not that NCSA would necessarily agree with each and every recommendation in every area the report covers.

The report was developed by active participation of a diverse group of representatives from industry, government, and the nonprofit sector. As it should, the findings and recommendations represent the great breadth and depth of the field. In NCSA's opinion, that's what gives the document credibility.

Moving together in unison is the best way to achieve our shared vision of making the Internet and cyberspace as safe and secure as possible for young people.

May 21, 2010

Statement Regarding the NTIA Online Safety and Technology Working Group's Final Report to Congress and the Secretary of Commerce

Verizon commends the Working Group for the high quality of its report on the state of Internet safety in the U.S. today. We applaud the fine work and research captured in the report and we agree with most of the recommendations. There are several additional points that Verizon believes Congress and the Administration need to take into account as they consider the current and future state of Internet safety:

- **Regulation would diminish, not improve, Internet safety.** The Internet is a global network of networks. The public Internet is made up of more than 25,000 interconnected networks owned and operated by corporations, governments, schools, and not-for-profits across the globe. Because not all these networks are located in the United States, local attempts to regulate the global Internet are at best ineffective and at worst detrimental to the proper functioning of the Internet. For example, attempts to regulate how network operators manage their networks may have the unintended consequence of tying their hands when it comes to responding the ever-changing real-time threats we see on today's Internet.

- **To the extent legislation or regulation of Internet safety is pursued, it should be only at the federal level**. The Internet is by its very nature an interstate (indeed, international) network. Standards for Internet safety, if they are to be adopted at all, should mirror the broad, cross-jurisdictional nature of the Internet. Conversely, if states were to set their own standards, the resulting patchwork of regulation would impose a confusing burden on the industry -- with as many as 54 different sets of requirements, creating uncertainty for consumers, parents, law enforcement, and industry participants.

- **Congress should take a "wait and see" approach before acting in the area of Internet safety.** Congress should first assess the impact of the more focused and efficient data preservation procedures enacted in the PROTECT Our Children Act before considering mandatory data retention or other provisions impacting Internet safety. Also, federal agencies have task forces and working groups looking at the efficacy of privacy laws to protect consumers when online and marketing to children online. The conclusions of these efforts need to be factored into any Congressional action on Internet safety.

Verizon takes its responsibility to protect its customers from Internet threats very seriously, just as we have long demonstrated our commitment to protecting customer privacy. We look forward to working with our industry partners to make the Internet a safer place for children, parents, and increasingly, seniors, in a cooperative and collaborative fashion. Verizon looks forward to participating in that dialog.

KEEPING THE INTERNET
OPEN • INNOVATIVE • FREE

www.cdt.org

CENTER FOR DEMOCRACY
& TECHNOLOGY

1634 I Street, NW
Suite 1100
Washington, DC 20006

P +1-202-637-9800
F +1-202-637-0968
E info@cdt.org

Statement of **John B. Morris, Jr.**
Center for Democracy & Technology

ONLINE SAFETY TECHNOLOGY WORKING GROUP

May 26, 2010

We commend the OSTWG participants for completing an important analysis of online safety issues, especially in light of the lack of resources available to the group to conduct any serious data gathering. We agree with the broad conclusion that a combination of education and technology tools are the most effective means that parents can use to protect their children online. The work of the OSTWG reinforces the conclusions of past blue ribbon panels that have endorsed education and technology tools.

A primary point of contention within the Working Group centered on the question of data retention – whether service providers should record and retain information about users' Internet use. Unsurprisingly, law enforcement participants support data retention, while civil liberties advocates and industry representatives believe that data retention poses serious privacy concerns. We believe that law enforcement can take advantage of other options for directing service providers to preserve information needed for specific investigations (as opposed to a broad mandate that required that information be retained about all users).

What is surprising, however, is the breadth of data retention sought in this report by law enforcement. The debate thus far over data retention has centered on possible requirements on Internet access providers for them to retain records of "IP address allocations," which could be used to link an e-mail or other online communication to a particular Internet subscriber. Even this type of proposal, which is focused on a narrow set of data retained only by a user's access provider, raises serious privacy and other concerns.

In this report, however, law enforcement is advocating for a radically broader and more invasive approach to data retention, in which any online service on the Internet which allows users to post any content, information, or comment would be required to keep track of every interaction with every visitor to their sites. The reach of this proposal is breathtaking and would require the tracking and storage of a vast amount of information documenting exactly where Internet users go and what they do online. This type of sweeping data retention would transform the Internet from an open forum for free speech to a massive surveillance system in which users would know that every move they make is recorded and potentially reviewable by the government. There are, as detailed in the report, significant policy problems with the sweeping data retention suggested here.

News Corporation

IN SUPPORT OF

Youth Safety on a Living Internet
Report of the Online Safety and Technology Working Group

For the past 20 years I have been focused on the safety, security, and privacy of individuals – as a prosecutor and a corporate executive. During this time, I have had the honor of providing counsel to or serving on different online safety task forces. Through News Corporation alone, I was involved in the Virginia and Washington State Attorneys General Youth Internet Safety Task Forces, the Berkman Center's Internet Safety Technical Task Force, and this OSTWG.

And as News Corporation's Chief Security Officer, I had the privilege of serving a company for whom the safety, security, and privacy of its online users has remained a top priority. On behalf of News Corporation, I congratulate the OSTWG for successfully completing a well-grounded and collaborative effort to evaluate industry efforts to promote a safer online environment for children. We thank the members for their time, effort, and dedication in bringing this report to fruition.

I also want to personally thank Anne Collier. As co-chair of the OSTWG, Anne was a sincere pleasure to partner with. Her dedication, strength of conviction, and safety acumen allowed us to jointly lead a group of experts from every facet of the safety ecosystem towards areas of true agreement and collaboration. During our tenure, we saw incredible leadership from Chris Bubb, Larry Magid, Michael McKeehan, and Adam Thierer, our subcommittee chairs that were given the challenging task of putting the pieces together for each area we focused on – and they did. To them, we offer a heartfelt thank you. Finally, we extend a sincere appreciation to NTIA and especially to Assistant Secretary Lawrence Strickling, Danny Weitzner, Tim Sloan, and Joe Gattuso for the tremendous support this past year.

One recurring theme has become indelible in the last several years – a holistic approach must be taken in order for us to have a significant impact on the online safety of our nation's youth. This report provides recommendations designed to lay the foundations for this holistic approach to prosper today and in the years to come. Simply put, child online safety solutions must be the result of active participation from every stakeholder in society. Only then can we succeed.

Online safety must remain a journey, not a destination.

Hemanshu Nigam
Co-Chair, OSTWG
Safety Advisor, News Corporation (former Chief Security Officer)

United States Telecom Association (USTelecom) Statement Regarding the Online Safety and Technology Working Group (OSTWG) Final Report to Congress

USTelecom thanks the OSTWG Co-Chairs, Hemanshu Nigam and Anne Collier for their leadership over the past year, as well as the individual members of the OSTWG for their joint efforts and individual contributions. As the premier trade association representing service providers and suppliers for the telecommunications industry, USTelecom was honored to be a part of this group and remains committed to ensuring that families and children are safe and secure online. The OSTWG was fortunate to have representatives from nearly every facet of the child online safety ecosystem represented, including the Internet industry, child safety advocacy organizations, educational communities, and the government, and law enforcement communities. Despite the broad range of membership in the OSTWG, there was substantial consensus regarding the current status of online safety efforts.

The OSTWG agreed that no "silver bullet" can address the many facets of youth online safety. Parents, educators, and others are utilizing a broad array of tools that include educational resources, parental control technologies, family and school policies, and government education efforts. USTelecom agrees with the OSTWG's assessment that "any solution to online safety must be holistic in nature and multi-dimensional in breadth." Many of USTelecom's members are at the forefront of providing consumers with the tools they need to ensure that families and children have a safe and secure online experience.

USTelecom's member companies also remain dedicated to the fight against child exploitation on the Internet. We applaud the efforts of our partners in this effort, including the National Center for Missing and Exploited Children (NCMEC) and the law enforcement community. Thanks in part to these ongoing collaborative efforts, recent changes to Federal law, the recommendations contained in the report, USTelecom is optimistic that these factors will help accelerate investigative efforts and spur additional criminal prosecutions of child pornography offenders.

While the report noted the contentious aspect of data retention, USTelecom supports the subcommittee's ultimate recommendations, including increased communication between law enforcement and network providers. Moving forward, we look forward to active dialog with our law enforcement partners and other stakeholders to achieve similar goals. USTelecom believes such active dialogue will result in achieving the appropriate balance between the legitimate needs of law enforcement, consumers' rightful privacy concerns, and the valid operational and business concerns of network providers.

USTelecom is committed to fulfilling the OSTWG's recommendation to "fill the prescription." Our member companies take very seriously their shared responsibility to keep families and children safe and secure in the online environment. We look forward to continuing our work with government, industry and non-profit partners to improve upon the practices and offerings to make the Internet a safer place for families and children.

607 14th Street NW, Suite 400 • Washington, DC 20005-2164 • 202.326.7300 T • 202.326.7333 F • www.ustelecom.org

The National Center for Missing & Exploited Children (NCMEC) is grateful for the opportunity to participate in the Online Safety and Technology Working Group (OSTWG). The OSTWG Members represent a wide range of key constituencies and perspectives on these issues. The diversity of the Members resulted in lively and productive exchanges on such topics as Internet safety education, sexting, data retention, safety tools and industry efforts regarding sexually abusive images of children.

We thank Anne Collier and Hemanshu Nigam for their leadership, the subcommittee chairs and all the Members for dedicating their time and effort to this report.

NCMEC recognizes that procedural limitations on the OSTWG subcommittees, specifically their inability to conduct surveys or new research, hindered their work. The OSTWG subcommittees would have likely been able to achieve a more complete understanding of the issues and subsequently provide more robust recommendations if they had been able to conduct surveys. Instead, the group had to rely on research that is more than 5 years old and has already been reviewed by a prior task group (the Internet Safety Technical Task Force). This report would have benefitted significantly from more current research on the issues, whether conducted by OSTWG or other groups. Technology, and how people use it changes rapidly, which reinforces the critical need for up-to-date research on these issues. Policymakers should consider only the most recent data in drafting solutions to Internet-facilitated problems.

NCMEC is troubled by the report's emphasis on the prevalence of peer-on-peer predation. We are concerned that this focus seems to discount the threat of adult predation and the impact that peer-on-peer predation has on child victims. Regardless of the source of the predation, any unwanted sexual solicitation should be treated as a serious problem by parents/guardians, Internet safety advocates and policymakers. We urge policymakers to treat online peer-on-peer predation with the same degree of concern as cyberbullying, another type of malicious peer-on-peer conduct.

In addition, while children are being enticed online by other children, it is important not to diminish the fact that children are being enticed into sexual activity by adults in significant numbers. Reports to NCMEC's CyberTipline regarding enticement have increased 714% since 1998. There is an urgent need for current research on this issue. We urge policymakers to seek out a range of sources, including industry and law enforcement, to quantify the scope of this problem.

OSTWG covered a wide range of issues and, in many areas, has provided strong recommendations for consideration. We applaud the Members for their efforts and commitment. The limitation of NCMEC's comments to these discrete issues should not be considered to be an endorsement of the report in its entirety.

CTIA Commends the National Telecommunications & Information Administration's Working Group Report on Online Safety Tools and Initiatives

CTIA – The Wireless Association®[1] commends the U.S. Department of Commerce National Telecommunications & Information Administration's ("NTIA") Online Safety & Technology Working Group ("OSTWG") for their efforts in outlining the communications industry's initiatives to promote responsible online use among children and teens. While the OSTWG report describes the inappropriate and irresponsible ways children and teens may be using online technology, including texting while driving, sexting, and cyberbullying, CTIA believes the report demonstrates the wireless industry's commitment to offer tools that are providing parents with choice and control over the content and services their children utilize. The OSTWG report also highlights industry's efforts to support law enforcement in the eradication of child pornography, and cooperate with lawful requests for information from law enforcement while protecting consumer privacy and constitutional rights.

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. Today, mobile technology offers many educational benefits to children and teens, including mLearning and thousands of educational "apps" focused on language and literacy programs, news, and in-class teaching opportunities.[2]

CTIA and the wireless industry are taking steps to educate kids, parents and teachers about responsible wireless use in these evolving mobile environments. For example, CTIA and The Wireless Foundation recently announced *Be Smart. Be Fair. Be Safe: Responsible Wireless Use* (http://www.besmartwireless.com/), a national education campaign focused on equipping parents and caregivers with the necessary materials and tools to help kids use their wireless devices responsibly. In addition, CTIA has developed a number of voluntary best practices and guidelines under which carriers and manufacturers agree to provide significant protections for consumers and, most specifically, children. 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.[3]

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 NTIA 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 America's youth about responsible wireless use.

---

[1]CTIA – The Wireless Association® (www.ctia.org) is the international association for the wireless telecommunications industry, representing carriers, manufacturers and wireless Internet providers.

[2] Comments of CTIA-The Wireless Association, FCC, MB Docket No. 09-194 (February 24, 2010), *available at* http://fjallfoss.fcc.gov/ecfs/document/view?id=7020390790.

[3]CTIA, Business Resources, Wireless Internet Caucus, *Best Practices and Guidelines for Location Based Services,* http://www.ctia.org/business_resources/wic/index.cfm/AID/11300 (last visited May 18, 2010).

Adam Thierer
President,
The Progress & Freedom Foundation (www.PFF.org)

It has been a privilege to serve on this working group and to direct its subcommittee on parental control technologies. I greatly appreciate being given this opportunity, and it was a joy to work with so many brilliant experts, advocates, academics, and industry leaders who were uniformly dedicated to making our children's online experiences safer and more satisfying.

Consistent with what other blue ribbon working groups, task forces, and various experts have found many times before, OSTWG members have generally concluded that there is no silver-bullet technical solution to online child safety concerns. Instead – and again in agreement with previous research and reports – we have concluded that a diverse toolbox must be brought to bear on these problems and concerns. In essence, we have generally endorsed what I have elsewhere referred to as the "3-E" solution, which stands for Education, Empowerment, and Enforcement:

- ***E**ducation and mentoring* is the most essential part of the solution. We can – and must – do more as parents and as a society to guide our children's behavior and choices online.
- ***E**mpowerment* is also essential, however. We can provide parents with more and better tools to make informed decisions about media and communications tools in their lives and the lives of their children. But technical tools can only supplement – they can never supplant – education, parental guidance, and better mentoring.
- ***E**nforcement* of laws and policies is also essential. We need to make sure that law enforcement officials have the resources they need to carry out the important task of protecting children from legitimate online threats.

The OSTWG task force report puts meat on the bones of this "3-E" model and provides the public and policymakers with a wealth of sound advice regarding the steps that should be taken to ensure our kids have safer online experiences.

Importantly, we have accomplished this without resorting to the "moral panic" tone that some have adopted when approaching these issues and concerns. While there are serious challenges and concerns surrounding discussions about child safety, it's important to acknowledge the important benefits of new media and communications technologies to us and our children. We have done so here.

Moreover, we have been careful not to try to unsettle any settled First Amendment law. One of the most regrettable developments of the past 15 years is that so much time has been wasted passing and then litigating legislative and regulatory enactments that have been so clearly unconstitutional under the First Amendment. If the time and resources that were squandered in those legal skirmishes would have instead been plowed into education, empowerment, and enforcement-based efforts, it could have made a lasting difference. More generally, we should always remember the sage advice offered by the Supreme Court in 2000: "Technology expands the capacity to choose; and it denies the potential of this revolution if we assume the Government is best positioned to make these choices for us."

We have charted a sensible way forward in this report that should hopefully avoid those problems. It is my hope that policymakers take our findings and recommendations seriously and adopt the sort of constructive, practical approach we have outlined here.

Evolve the Internet to Protect Families

CP80.org and ThinkAtomic appreciate the opportunity to serve on OSTWG and thank the other members, especially the co-chairs and subcommittee chairs, for their contributions and hard work. While there are many conclusions in the OSTWG Report with which we agree, especially those urging greater education of parents and children, additional factors should be taken into account by Congress and the Administration. Specific mention of certain issues in this Addendum should not be taken to mean that we necessarily agree with any other aspects of the Report.

The primary problem with the OSTWG effort is we were unable to conduct surveys or other data gathering. Especially in the parental controls subcommittee, we did none of our own research and did little to incorporate existing data to support the generalizations and opinions of OSTWG members. For instance, we heard descriptions of various products promoted by the industry, but we made no attempt to do a complete review of what is and is not available, and we made no findings on the effectiveness of any parental control device or program. This kind of analysis was, however, recently conducted by the Berkman Center for Internet and Society. Because OSTWG was unable to conduct our own evaluations, the findings of this study provide better information on parental controls.

We agree there is no "silver bullet" solution, but parents deserve an effective blocking option for protecting children online. While a broad variety of tools are indeed available, we believe this report overstates their effectiveness and avoids the frank truth about the problems of each kind of tool. Moreover, the increasing use of "proxy" sites, the ready availability of filter-circumventing advice (as on Wikipedia), and especially the onset of "cloud" services have nullified parental efforts. Something is clearly not working when only a little over "half (54 %) of internet-connected families with teens now use filters." Especially disconcerting is the ability of minors to access unfiltered Internet with mobile devices almost everywhere. "[E]ffective filtering systems [are not] widely in place on cell phones with internet access or iPods . . . , despite the popularity of such contemporary media among adolescents."

Parents deserve the support of government in making decisions about the education of their children. The laws in place in the real world to protect children largely do not apply online, and where the law does apply, such as the prohibition on obscenity and child porn, law enforcement are given insufficient resources to keep up. Government needs to do more than wait and see, conduct studies, and educate children on avoiding harm. Illegal activity on the Internet needs to be stopped. Certainly, we are entitled to minimum data retention requirements similar to those for telephone records and drivers and vehicle licensing.

While the industry recognizes protecting minors is a "high priority," greater scrutiny needs to be focused on exactly what measures are being taken to assure results, especially, as the Report acknowledges, now that the industry heeds calls for even greater lack of accountability in the name of privacy.

Ralph Yarro III
Chairman, Board of Trustees
The CP80 Foundation