



Five Online Safety Task Forces Agree: Education, Empowerment & Self-Regulation Are the Answer

by Adam Thierer^{*}

Public policy debates about online child safety have raged since the earliest days of the Internet. Concerns about underage access to objectionable *content* (specifically pornography) drove early “Web 1.0” efforts to regulate the Internet, and it continues to be the topic of much discussion today. With the rise of the more interactive “Web 2.0” environment, however, objectionable *contact and communications* (harassment, cyberbullying, predation, etc.) have become a more significant concern and is now driving many regulatory proposals.¹

Over the past decade, five major online safety task forces or blue ribbon commissions have been convened to study these concerns, determine their severity, and consider what should be done to address them. Two of these task forces were convened in the United States and issued reports in 2000 and 2002. Another was commissioned by the British government in 2007 and issued in a major report in March 2008. Finally, two additional online safety task forces were formed in the U.S. in 2008 and concluded their work, respectively, in January and July of 2009.

Altogether, these five task forces heard from hundreds of experts and produced thousands of pages of testimony and reports on a wide variety of issues related to online child safety. While each of these task forces had different origins and unique membership, what is striking about them is the general unanimity of their conclusions. Among the common themes or recommendations of these five task forces:

- **Education is the primary solution** to most online child safety concerns. These task forces consistently stressed the importance of media literacy, awareness-building efforts, public service announcements, targeted intervention techniques, and better

* Adam Thierer (athierer@pff.org) is a Senior Fellow with PFF and the Director of The Progress & Freedom Foundation (PFF) Center for Digital Media Freedom. He served as member of the Internet Safety Technical Task Force and the “PointSmart. ClickSafe.” task forces highlighted in this report. He also served as an advisor to the “Byron Commission” task force discussed herein. Finally, he was recently appointed as a member of the new Online Safety Technical Working Group (OSTWG), which was created by Congress to study these same issues. The views expressed here are his own, and are not necessarily the views of the PFF board, other PFF fellows or staff, or any of the task forces on which he has served.

¹ For a more extensive discussion of how these debates have played out over the past decade, see Adam Thierer, The Progress & Freedom Foundation, *Parental Controls and Online Child Protection: A Survey of Tools and Methods*, Special Report, Ver. 3.1, Fall 2008, www.pff.org/parentalcontrols/index.html

mentoring and parenting strategies.

- **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.
- **Empowering parents and guardians with a diverse array of tools**, however, can help families, caretakers, and schools to exercise more control over online content and communications.
- Technological tools and parental controls are most effective as part of a **“layered” approach to child safety** that views them as one of many strategies or solutions.
- The best technical control measures are those that work in tandem with educational strategies 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.**
- **Industry should formulate 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 often 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.
- 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. **Additional resources for education** and awareness-building efforts are also crucial. Finally, governments should **ensure appropriate penalties are in place to punish serious crimes** against children and also **make sure law enforcement agencies have adequate resources** to police crimes and punish wrong-doers.

The consistency of these findings from those five previous task forces is important and it should guide future discussions among policymakers, the press, and the general public regarding online child safety.²

The findings are particularly relevant today since Congress and the Obama Administration are

² Importantly, this is also the general approach that many other child safety experts and authors have taken when addressing these issues. For example, see Nancy E. Willard, *Cyber-Safe Kids, Cyber-Savvy Teens* (San Francisco, CA: Jossey-Bass, 2007), www.cskcst.com; Larry Magid and Anne Collier, *MySpace Unraveled: A Parent's Guide to Teen Social Networking* (Berkeley, CA: Peachtree Press, 2007), www.myspaceunraveled.com; Sharon Miller Cindrich, *e-Parenting: Keeping Up with Your Tech-Savvy Kids* (New York: Random House Reference, 2007), www.pluggedinparent.com; Jason Illian, *MySpace, MyKids: A Parent's Guide to Protecting Your Kids and Navigating MySpace.com* (Eugene, OR: Harvest House Publishers, 2007); Linda Criddle, *Look Both Ways: Help Protect Your Family on the Internet* (Redmond, WA: Microsoft Press, 2006), <http://look-both-ways.com/about/toc.htm>; Gregory S. Smith, *How to Protect Your Children on the Internet: A Road Map for Parents and Teachers* (Westport, CT: Praeger, 2007), www.gregoryssmith.com.

actively studying these issues. For example, three federal agencies are currently exploring various aspects of this debate:

- **NTIA (OSTWG):** The “Protecting Children in the 21st Century Act,” which was signed into law by President Bush in 2008 as part of the “Broadband Data Services Improvement Act,”³ authorized the creation of an Online Safety and Technology Working Group (OSTWG). The National Telecommunications and Information Administration (NTIA) at the U.S. Department of Commerce, which is overseeing the effort, has appointed 35 members to serve 15-month terms to study the status of industry efforts to promote online safety, best practices among industry leaders, the market for parental control technologies, and assistance to law enforcement in cases of online child abuse. The U.S. Department of Justice, the U.S. Department of Education, the Federal Communications Commission, and the Federal Trade Commission all have delegates serving on the working group. OSTWG began its work in early June 2009 and is due to report back to Congress one year later.⁴
- **FTC:** That same bill that created the OSTWG, also requires that the Federal Trade Commission (FTC) “carry out a nationwide program to increase public awareness and provide education” to promote safer Internet use. “The program shall utilize existing resources and efforts of the Federal Government, State and local governments, nonprofit organizations, private technology and financial companies, Internet service providers, World Wide Web-based resources, and other appropriate entities, that includes (1) identifying, promoting, and encouraging best practices for Internet safety; (2) establishing and carrying out a national outreach and education campaign regarding Internet safety utilizing various media and Internet-based resources; (3) facilitating access to, and the exchange of, information regarding Internet safety to promote up-to-date knowledge regarding current issues; and, (4) facilitating access to Internet safety education and public awareness efforts the Commission considers appropriate by States, units of local government, schools, police departments, nonprofit organizations, and other appropriate entities.”
- **FCC:** Pursuant to the requirements set forth in the Child Safe Viewing Act of 2007,⁵ the Federal Communications Commission (FCC) launched a *Notice of Inquiry* in March 2009

³ Broadband Data Services Improvement Act of 2008, P.L. 110-385, 110th Congress.

⁴ See Leslie Cantu, *Newest Online Safety Group Will Report on Industry Efforts*, Washington Internet Daily, Vol. 10 No. 107, June 5, 2009; Larry Magid, *Federal Panel Takes a Fresh Look at Kids’ Internet Safety*, San Jose Mercury News, www.mercurynews.com/business/ci_12522370?nclick_check=1; Adam Thierer, The Progress & Freedom Foundation, *Online Safety Technology Working Group (OSTWG) Is Underway*, PFF Blog, June 4, 2009, http://blog.pff.org/archives/2009/06/online_safety_technology_working_group_ostwg_is_un.html

⁵ Child Safe Viewing Act of 2007, P.L. 110-452, 110th Congress. Also see Adam Thierer, The Progress & Freedom Foundation, *“Child Safe Viewing Act” (S. 602) Signed by President Bush*, PFF Blog, Dec. 2, 2008, http://blog.pff.org/archives/2008/12/child_safe_view.html

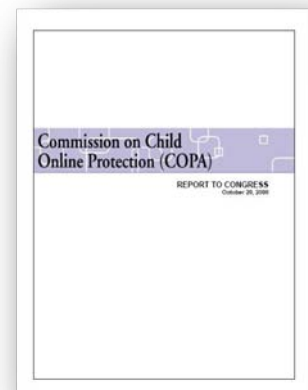
to survey the parental controls marketplace.⁶ Specifically, the Act requires the FCC to examine: (1) the existence and availability of advanced blocking technologies that are compatible with various communications devices or platforms; (2) methods of encouraging the development, deployment, and use of such technology by parents that do not affect the packaging or pricing of a content provider's offering; and, (3) the existence, availability, and use of parental empowerment tools and initiatives already in the market. The proceeding prompted a diverse assortment of filings from industry and non-profit groups discussing the technologies and rating systems on the market today.⁷ The Act requires that the FCC issue a report to Congress about these technologies no later than August 29, 2009.⁸

As these agencies, future task forces, academics, and others continue to study these issues, they should keep the findings of past online safety task forces in mind. What follows is an expanded chronological discussion of the major findings of each of the five major online safety task forces that have been convened since 2000.

2000 – Commission on Online Child Protection (“COPA Commission”)

The COPA Commission was formed pursuant to the federal Child Online Protection Act, which Congress passed in October 1998.⁹ The Act mandated all website operators to restrict access to material deemed “harmful to minors” under the age of 17. Thus, in order to identify minors, the law required some form of age verification of *all* users who attempt to access such content. After a decade-long court battle over the constitutionality of COPA, however, the U.S. Supreme Court in January 2009 rejected the government’s latest request to revive the law, meaning it is likely dead.¹⁰

The COPA Commission, however, was unaffected by this judicial battle and its report remains the most important legacy of the law. Congress asked the COPA Commission to study methods to help



⁶ Federal Communications Commission, Notice of Inquiry *In the Matter of Implementation of the Child Safe Viewing Act; Examination of Parental Control Technologies for Video or Audio Programming*, FCC 09-14, MB Docket No. 09-26, March 2, 2009 (hereinafter FCC, Child Safe Viewing Act Notice).

⁷ See Adam Thierer, The Progress & Freedom Foundation, *Major Filings in FCC's 'Child Safe Viewing Act' Notice of Inquiry*, PFF Blog, Apr. 20, 2009, http://blog.pff.org/archives/2009/04/major_filings_in_fccs_child_safe_viewing_act_notic.html.

⁸ For more discussion of the possible implications of this proceeding, see Adam Thierer, The Progress & Freedom Foundation, *Dawn of Convergence-Era Content Regulation at the FCC? 'Child Safe Viewing Act' NOI Launched*, PFF Blog, March 3, 2009, http://blog.pff.org/archives/2009/03/dawn_of_convergence-era_content_regulation_at_the.html.

⁹ COPA Commission, *Report to Congress*, October 20, 2000, www.copacommission.org.

¹⁰ See Adam Thierer, The Progress & Freedom Foundation, *Closing the Book on COPA*, PFF Blog, Jan. 21, 2009, http://blog.pff.org/archives/2009/01/closing_the_book.html.

reduce access by minors to certain sexually explicit material online. Congress directed the Commission to evaluate the accessibility, cost, and effectiveness of protective technologies and methods, as well as their possible effects on privacy, First Amendment values and law enforcement. The Commission was chaired by Donald Telage, then Executive Advisor for Global Internet Strategy for Network Solutions Inc., and it had 18 members from academia, government, and industry. After hearing from a diverse array of parties and considering a wide range of possible solutions,¹¹ the COPA Commission concluded that:

no single technology or method will effectively protect children from harmful material online. Rather, the Commission determined that a combination of public education, consumer empowerment technologies and methods, increased enforcement of existing laws, and industry action are needed to address this concern.¹²

The COPA Commission also made specific recommendations concerning education, law enforcement and industry action, which are listed in Exhibit 1.¹³ The clear conclusion of the COPA Commission was that a layered, multi-faceted approach to online safety was essential. Education, empowerment, and targeted law enforcement strategies were the key. Finally, the COPA Commission helped highlight for policymakers “the unique characteristics of the Internet and its impact on the ability to protect children”:

The Internet’s technical architecture creates new challenges as well as opportunities for children and families. Material published on the Internet may originate anywhere, presenting challenges to the application of the law of any single jurisdiction. Methods for protecting children in the U.S. must take into account this global nature of the Internet. In addition, thousands of access providers and millions of potential publishers provide content online. Methods to protect children from content harmful to minors must be effective in this diverse and decentralized environment, including the full range of Internet activity such as the Web, email, chat, instant messaging, and newsgroups. The Internet is also rapidly changing and converging with other, more traditional media. Effective protections for children must accommodate the Internet’s convergence with other media and extend to new technologies and services offered on the Internet, [since] ... unlike one-way broadcast media, the Internet is inherently multi-directional and interactive.¹⁴

¹¹ The Commission evaluated: filtering and blocking services; labeling and rating systems; age verification efforts; the possibility of a new top-level domain for harmful to minors material; “green” spaces containing only child-appropriate materials; Internet monitoring and time-limiting technologies; acceptable use policies and family contracts; online resources providing access to protective technologies and methods; and options for increased prosecution against illegal online material. *Id.* at 14.

¹² *Id.* at 9.

¹³ *Id.* at 9-10.

¹⁴ *Id.* at 13.

Exhibit 1: COPA Commission Recommendations**Public Education:**

- Government and the private sector should undertake a major education campaign to promote public awareness of technologies and methods available to protect children online.
- Government and industry should effectively promote acceptable use policies.

Consumer Empowerment Efforts:

- Resources should be allocated for the independent evaluation of child protection technologies and to provide reports to the public about the capabilities of these technologies.
- Industry should take steps to improve child protection mechanisms, and make them more accessible online.
- A broad, national, private sector conversation should be encouraged on the development of next-generation systems for labeling, rating, and identifying content reflecting the convergence of old and new media.
- Government should encourage the use of technology in efforts to make children's experience of the Internet safe and useful.

Law Enforcement:

- Government at all levels should fund, with significant new money, aggressive programs to investigate, prosecute, and report violations of federal and state obscenity laws, including efforts that emphasize the protection of children from accessing materials illegal under current state and federal obscenity law.
- State and federal law enforcement should make available a list, without images, of Usenet newsgroups, IP addresses, World Wide Web sites or other Internet sources that have been found to contain child pornography or where convictions have been obtained involving obscene material.
- Federal agencies, pursuant to further Congressional rulemaking authority as needed, should consider greater enforcement and possibly rulemaking to discourage deceptive or unfair practices that entice children to view obscene materials, including the practices of "mousetrapping" and deceptive metatagging.
- Government should provide new money to address international aspects of Internet crime, including both obscenity and child pornography.

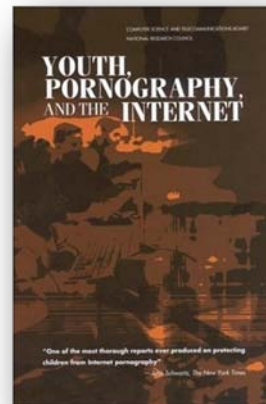
Industry Action:

- The ISP industry should voluntarily undertake "best practices" to protect minors.
- The online commercial adult industry should voluntarily take steps to restrict minors' ready access to adult content.

2002 – Youth, Pornography, and the Internet (“Thornburgh Commission”)

In 2001, a blue-ribbon panel of experts was convened by the National Research Council (NRC) of the National Academy of Sciences to study how best to protect children from objectionable online material, namely, pornography. Congress had passed legislation in November 1998 requiring that the NRC “conduct a study of computer-based technologies and other approaches to the problem of the availability of pornographic material to children on the Internet.”¹⁵

Under the leadership of former U.S. Attorney General Richard Thornburgh, in 2002, the group produced a massive, 450-page report (*Youth, Pornography, and the Internet*) that discussed a comprehensive collection of strategies for dealing with potentially objectionable media content or online dangers.¹⁶ The Thornburgh Commission used a compelling metaphor to explain why education was the most essential strategy for addressing these concerns:



Technology—in the form of fences around pools, pool alarms, and locks—can help protect children from drowning in swimming pools. However, teaching a child to swim—and when to avoid pools—is a far safer approach than relying on locks, fences, and alarms to prevent him or her from drowning. Does this mean that parents should not buy fences, alarms, or locks? Of course not—because they do provide some benefit. But parents cannot rely exclusively on those devices to keep their children safe from drowning, and most parents recognize that a child who knows how to swim is less likely to be harmed than one who does not. Furthermore, teaching a child to swim and to exercise good judgment about bodies of water to avoid has applicability and relevance far beyond swimming pools—as any parent who takes a child to the beach can testify.¹⁷

The report also included a lengthy chapter on “Social and Educational Strategies to Develop Personal and Community Responsibility,” which pointed out how “exclusive—or even primary—reliance on technological measures for protection would be an abdication of parental and community responsibility and is likely to be ineffective as well.”¹⁸ Education was the preferred approach because “technology often does not live up to its promises,” and “because technology changes rapidly for everyone, technology tools developed to solve problems exposed by other technological developments may quickly be rendered obsolete.”¹⁹

¹⁵ Title IX, Sec. 901 of The Protection of Children from Sexual Predators Act of 1998, Pub. Law 105-314.

¹⁶ 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/

¹⁷ *Id.* at 224.

¹⁸ *Id.* at 221.

¹⁹ *Id.* at 222.

The Thornburgh Commission also found that “Technology-based tools, such as filters, provide parents and other responsible adults with additional choices as to how best fulfill their responsibilities.”²⁰ In other words, technological tools and approaches could supplement educational strategies.²¹ However, the report also concluded, however, “there is no single or simple answer to controlling the access of minors to inappropriate material on the Web.”²² Thus, the Thornburgh Commission advocated a layered approach to the issue:

Though some might wish to think otherwise, no single approach—technical, legal, economic, or education—will be sufficient. Rather, an effective framework for protecting our children from inappropriate materials and experiences on the Internet will require a balanced composite of all these elements, and real progress will require forward movement on all these fronts.²³

2008 – Safer Children in a Digital World (“Byron Review”)

In September 2007, the British government asked Dr. Tanya Byron, a prominent British psychologist, to conduct an independent review of the risks to children from exposure to potentially harmful or inappropriate material on the Internet and in video games.

Dr. Byron delivered her report to the Prime Minister in March 2008: *Safer Children in a Digital World: The Report of the Byron Review*.²⁴ It reflected many of the same themes, and reached many of the same conclusions, as the U.S.-based reports mention herein. Again, there was a realization that there are no easy answers to these complicated issues:

There is no ‘silver bullet’. Neither Government nor industry can make the internet completely safe. The nature of the internet means that there will always be risks, and children and parents need to understand how to manage the risks of the internet.

As such, policies that claim to make the internet completely safe are undesirable because they discourage children and parents from taking an informed approach to



²⁰ *Id.* at 12.

²¹ “While technology and public policy have important roles to play, social and educational strategies that impart to children the character and values to exercise responsible choices about Internet use and the knowledge about how to cope with inappropriate material and experiences is central to promoting children’s safe Internet use.” *Id.* at 388.

²² *Id.* at 12.

²³ *Id.* at 13.

²⁴ *Safer Children in a Digital World: The Report of the Byron Review*, March 27, 2008, www.dcsf.gov.uk/byronreview. The complete final report can be found at: www.dcsf.gov.uk/byronreview/pdfs/Final%20Report%20Bookmarked.pdf.

managing the risks. At worst they can be dangerous – lulling parents into a false sense of security and leaving children exposed to a greater level of risk than they would otherwise be.²⁵

The Byron Review also emphasized the importance of education and building resiliency:

Just like in the offline world, no amount of effort to reduce potential risks to children will eliminate those risks completely. We cannot make the internet completely safe. Because of this, we must also build children’s *resilience* to the material to which they may be exposed so that they have the confidence and skills to navigate these new media waters more safely.²⁶

[And] crucial and central to this issue is a strong commitment to changing behavior through a sustained information and education strategy. This should focus on raising the knowledge, skills and understanding around e-safety of children, parents and other responsible adults.²⁷

The Byron Review recommended a comprehensive information and education strategy through a partnership of government, schools, child safety experts, and industry. It also recommended that government policy be more tightly coordinated by a new UK Council for Child Internet Safety, which would report to the Prime Minister. Finally, the Byron Review outlined a variety of industry best practices that could help parents and children achieve greater online safety.

2009 – Internet Safety Technical Task Force (ISTTF)

On January 14th, 2008, social networking website operator MySpace.com announced a joint effort with 49 state Attorneys General (AGs) aimed at better protecting children online. As part their “Joint Statement on Key Principles of Social Networking Safety,” MySpace promised the AGs it would create new online safety tools, improve education efforts, and expand its cooperation with law enforcement.²⁸ They also agreed to create an industry-wide Internet Safety Technical Task Force (ISTTF) to study online safety tools, including a review of online identity authentication technology.²⁹ The ISTTF, which was chaired by Harvard University



²⁵ *Id.* at 81.

²⁶ *Id.* at 5.

²⁷ *Id.* at 7.

²⁸ *MySpace and Attorneys General Announce Joint Effort to Promote Industry-Wide Internet Safety Principles*, News Corp., Press Release, January 14, 2008, www.newscorp.com/news/news_363.html

²⁹ Adam Thierer, The Progress & Freedom Foundation, *The MySpace-AG Agreement: A Model Code of Conduct for Social Networking?* Progress on Point 15.1, Jan. 2008, www.pff.org/issues-pubs/pops/pop15.1myspaceAGagreement.pdf

law professor John Palfrey, the Co-Director of Harvard's Berkman Center for Internet & Society, included representatives from many child safety groups, non-profit organizations, and Internet companies.

The ISTTF convened a Research Advisory Board (RAB), which brought together leading academic researchers in the field of child safety and child development and a Technical Advisory Board (TAB), which included some of America's leading digital technologists and computer scientists, who reviewed child safety technologies submitted to the ISTTF. The RAB's literature review³⁰ and TAB's assessment of technologies³¹ were the most detailed assessments of these issues to date. They both represent amazing achievements in their respective arenas.

On December 31, 2008, the ISTTF issued its final report, *Enhancing Child Safety & Online Technologies*.³² Consistent with previous task force reports, the ISTTF found that "there is no one technological solution or specific combination of technological solutions to the problem of online safety for minors."³³ And, while the ISTTF was, "optimistic about the development of technologies to enhance protections for minors online and to support institutions and individuals involved in protecting minors," it ultimately "caution[ed] against overreliance on technology in isolation or on a single technological approach".³⁴

Instead, a combination of technologies, in concert with parental oversight, education, social services, law enforcement, and sound policies by social network sites and service providers may assist in addressing specific problems that minors face online. All stakeholders must continue to work in a cooperative and collaborative manner, sharing information and ideas to achieve the common goal of making the Internet as safe as possible for minors.³⁵

Finally, the ISTTF recognized the importance of providing adequate resources to law enforcement, schools, and social service organizations so they can better deal with child safety concerns:

To complement the use of technology, greater resources should be allocated: to schools, libraries, and other community organizations to assist them in adopting risk management policies and in providing education about online safety issues; to law

³⁰ http://cyber.law.harvard.edu/sites/cyber.law.harvard.edu/files/ISTTF_Final_Report-APPENDIX_C_Lit_Review_121808.pdf

³¹ http://cyber.law.harvard.edu/sites/cyber.law.harvard.edu/files/ISTTF_Final_Report-APPENDIX_D_TAB_and_EXHIBITS.pdf

³² 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 10, <http://cyber.law.harvard.edu/pubrelease/isttf>

³³ *Id.* at 6

³⁴ *Id.*

³⁵ *Id.*

enforcement for training and developing technology tools, and to enhance community policing efforts around youth online safety; and to social services and mental health professionals who focus on minors and their families, so that they can extend their expertise to online spaces and work with law enforcement and the Internet community to develop a unified approach for identifying at-risk youth and intervening before risky behavior results in danger.³⁶

2009 – “Point Smart. Click Safe.” Blue Ribbon Working Group

In June 2007, the National Cable & Telecommunications Association (NCTA), the principal trade association of the cable industry in the United States, announced “Cable Puts You in Control: PointSmart. ClickSafe.”³⁷ a new campaign by its members to offer parents assistance in keeping their children safe online.³⁸

As part of the initiative the NCTA hosted a major online child safety summit and also announced the formation of the “Point Smart. Click Safe.” Blue Ribbon Working Group in partnership with the Internet KeepSafe Coalition (iKeepSafe) and Common Sense Media. These three organizations, along with the cable industry’s “Cable in the Classroom” program, agreed to bring together a collection of online safety experts from many disciplines to study these issues and develop a set of “best practice” recommendations that could be implemented across the Internet industry.



In July 2009, the working group produced its final report.³⁹ In line with what previous task forces found, the “Point Smart. Click Safe.” Blue Ribbon Working Group concluded that:

Ensuring children’s online safety is a difficult and complex task that calls for input from and action by a wide variety of stakeholders. There is no “silver bullet”—no single technology or approach that has proved effective. Rather, what is required is:

- A combination of different technologies,
- Continuing digital literacy education for parents, educators, and children, and
- Active participation by all concerned companies, groups and individuals.

³⁶ *Supra* note 32 at 6.

³⁷ www.pointsmartclicksafe.org

³⁸ Adam Thierer, The Progress & Freedom Foundation, *Cable’s Commitment to Online Safety*, Progress Snapshot 3.7 June 2007, www.pff.org/issues-pubs/ps/2007/ps3.7cablecodeconduct.pdf.

³⁹ www.pointsmartreport.org

Similarly, a singular focus on safety is insufficient. Children must learn to minimize risks but also learn appropriate and ethical behaviors in this digital world. In addition, they need an understanding of media literacy, in order to be able to think critically about the content they consume and increasingly create. Therefore, best practices must be part of a larger effort to provide an entertaining, educational, and safe experience for children.

Again, the major contribution of this task force was its focus on detailed industry best practices that various online providers could adopt to help parents, policymakers, and law enforcement better keep kids safe online. As the working group's final report noted:

It should be easy for parents and others to find clear and simple explanations of what information and safety elements exist, how they function, and what a user can do in various circumstances. Therefore, best operating practices should:

- Use clear and common language,
- Be consistent and transparent, and
- Provide information and tools that can vary by age and stage of the user.

These best operating practices should be crafted so that they can be:

- Modified for a specific service or application (e.g. ISP, blog, chat, social network),
- Scaled based on the number of intended or actual users,
- Designed and created as part of the product development cycle, and
- Continuously updated to reflect growth and change in the application or service.

The task force then outlined several tools and strategies that industries could use to accomplish these goals. These "Recommendations for Best Practices" are summarized in Exhibit 2.

Exhibit 2: “Point Smart. Click Safe.” Recommendations for Best Practice

Before Children Go Online

1. Education and information

Basic information and education about the digital landscape must be in place and available to all children, parents, educators, and caregivers so they can understand the various risks, what constitutes appropriate behavior in different online spaces, and what options they have in services and terms of use. In addition, children need to learn how to use the technology efficiently, effectively and ethically so that they can participate fully in social, economic and civic life in the digital age. Best Practices should also encourage and empower parents, educators, and caregivers to understand the technology so they can make informed initial and ongoing choices for their children’s safety and security.

We recommend the following:

- 1.1 Provide access to information that will educate parents, educators, and children about media literacy and ethical digital citizenship, and help them think critically about the content consumed and created on the Internet.
- 1.2 Make safety information for users, parents, and caregivers prominent, easily accessible, and clear.
- 1.3 Provide information that is easy to find and access from the home page, available during registration, and that can also be found in other appropriate places within the Web site or service.
- 1.4 Include specific information or FAQs about the services offered by the provider, especially safety tools and how to use them (e.g., conducting a safe search, setting filtering options, defining and setting appropriate privacy levels).
- 1.5 Provide links to additional resources that offer relevant safety and security information.
- 1.6 To make messages about online safety clear and easily recognizable to a variety of users, consider using consistent themes, and common words and phrases. Provide messages in multiple languages as appropriate.
- 1.7 Consider display of an icon on Web sites or services that denotes meaningful participation in Best Practice efforts for children's online safety.

2. Registration/creation of user profiles

We recommend the following:

- 2.1 Provide a clear explanation of how information collected at registration and set up will be used, what is public vs. private on the site, and a user’s ability to modify, hide, and prevent access to user information.
- 2.2 Make safety information available during the registration process, prominent from the homepage and in appropriate places within the service (e.g. welcome email/message, point of sale information).
- 2.3 Provide information in the terms and conditions and elsewhere that defines acceptable behavior, states that users are not anonymous and can be traced, and details the consequences of violating the standards of behavior.
- 2.4 Provide notice that violating terms or conditions will result in specific consequences, including legal ones if required.

3. Identity authentication and age verification

The task force acknowledges that the issues of identity authentication and age verification remain substantial challenges for the Internet community due to a variety of concerns including privacy, accuracy, and the need for better technology in these areas. [...] Therefore we recommend the following:

- 3.1 Continue to explore age-verification and identity-authentication technologies and work to develop better safety and security solutions and technologies.

(cont.)

(cont.)

During a Child's Online Activities

Best Practices in this area should recommend how technologies can be used to define and control a child's digital activities and help parents establish the technology structure that they determine best meets their family values and needs as children grow and become more self-sufficient.

We recommend the following:

4. Content screening

- 4.1 Initially set defaults at a moderate level as a minimum, but instruct users in how to customize settings for their own needs.
- 4.2 Information should be provided about company policy on filtering, including the default settings, explanations of the meanings of different safety, security and filtering options (e.g., what is blocked by certain levels of filtering), how to make adjustments, and when settings might need to be reapplied (e.g., a new version).
- 4.3 Consider carefully the placement and highlighting of sites belonging to and designed by children and youth (e.g., a child's profile page could become a "safe zone," don't locate children's content near ads for adult-targeted materials).
- 4.4 Consider a "walled garden" approach when relevant with products aimed at children eight years of age and younger.

5. Safe searching

- 5.1 Include specific information about how to conduct a safe search, how to set filtering options, and an explanation of privacy settings.

When Problems Arise

6. To provide the best response to problems, we recommend:

- 6.1 Have in place a robust procedure, backed by appropriate systems and resources, to handle complaints. Ideally, each company should have an Internet-safety staff position or cross-functional team charged with supervising the procedures and resources and given the authority and resources to be effective.
- 6.2 Provide a reporting mechanism visible from all relevant pages or sections of a site or service.
- 6.3 Consider providing a designated page with relevant information and instructions about how to submit a report or complaint including:
 - How users can determine the appropriate individual or agency to contact when reporting a problem (e.g., customer service, law enforcement, or safety hotline) and links to these services.
 - What types of content and behaviors should be reported, the reporting procedure, and what supporting information might need to be included.
 - How to remove unwanted content or information from a user's page or profile.
 - How to cancel an account.
- 6.4 Cooperate with law enforcement, where applicable, and follow all relevant statutes.

Conclusion: We Should Heed the Collective Wisdom of the Past

While more study of online child safety issues is always welcome—including additional task forces or working groups if policymakers deem them necessary—thanks to the work of these past task forces, we now have better vision of what is needed to address online safety concerns. Education, empowerment, and targeted law enforcement efforts are the crucial ingredients to improving the safety of children online. And sensible industry self-regulation and best practices can help facilitate all those objectives.

Of these various strategies, however, education is the one with the most lasting impact. Education teaches lessons and builds resiliency, providing skills and strength that can last a lifetime. Specifically, education can help teach kids how to behave in—or respond to—a wide variety of situations.⁴⁰ The focus should be on encouraging “digital citizenship”⁴¹ and “social media literacy.”⁴²

If policymaker convene additional task forces or working groups in coming years, it would be wise to have them focus on devising and refining online safety educational methods and digital literacy efforts. In particular, focusing on how to integrate such education and literacy programs into existing K-12 education (including curriculum and professional development) would be a worthwhile undertaking. Of course, many groups are already busy studying how to do this, but if lawmakers feel compelled to bring together experts once more to study these issues, this sort of targeted focus on education and media literacy implementation would be welcome.

Importantly, it is worth noting that such education and media literacy-based approaches have the added benefit of remaining within the boundaries of the Constitution and the First Amendment. By adopting education and awareness-building approaches, government would not be seeking to restrict speech, but simply to better inform and empower parents regarding the parental control tools and techniques already at their disposal.⁴³ The courts have shown themselves to be amenable to such educational efforts, and not just in the case of online

⁴⁰ See Nancy Willard, *A Web 2.0 Approach to Internet Safety*, Education Week, Aug. 21, 2007, www.education-world.com/a_tech/columnists/willard/willard008.shtml

⁴¹ See Common Sense Media, *Digital Literacy and Citizenship in the 21st Century: Educating, Empowering, and Protecting America's Kids*, June 2009, www.common Sense Media.org/sites/default/files/CSM_digital_policy.pdf; Nancy Willard, Center for Safe and Responsible Internet Use, *Comprehensive Layered Approach to Address Digital Citizenship and Youth Risk Online*, Nov. 2008, www.cyberbully.org/PDFs/yrocomprehensiveapproach.pdf

⁴² See Anne Collier, Net Family News, *Social Media Literacy: The New Online Safety*, Feb. 27, 2009, www.netfamilynews.org/labels/new%20media%20literacy.html

⁴³ “Although government’s ability to regulate content may be weak, its ability to promote positive programming and media research is not. Government at all levels should fund the creation and evaluation of positive media initiatives such as public service campaigns to reduce risky behaviors and studies about educational programs that explore innovative uses of media.” Jeanne Brooks-Gunn and Elisabeth Hirschhorn Donahue, “Introducing the Issue,” in *Children and Electronic Media, The Future of Children*, Vol. 18, No. 1, Spring 2008, p. 8.

safety.⁴⁴ Thus, moving forward, lawmakers would be wise to focus on education-based strategies and initiatives, not regulatory ones.⁴⁵

If lawmakers instead enact more regulations aimed at banning certain types of online content,⁴⁶ or mandating unworkable solutions like mandatory online age verification,⁴⁷ those efforts will be bogged down in the courts for years to come. For example, the Child Online Protection Act (COPA) was passed by Congress in 1998 in an effort to restrict minors' access to adult-oriented websites. After a decade-long series of court battles about the constitutionality of the measure, in January 2009, the U.S. Supreme Court rejected the government's latest request to revive COPA, meaning it is likely dead.⁴⁸ If all the money and resources that were spent litigating COPA had instead been used for digital media literacy and online safety campaigns, it could have produced concrete, lasting results.

In sum, education, not regulation, represents the best approach to addressing content concerns about online child safety. But user empowerment, industry self-regulation, and increased resources for targeted law enforcement efforts are also essential.

⁴⁴ In the video game context, courts have noted the education typically provides the more sensible, and constitution, method of dealing with concerns about access to objectionable content.

⁴⁵ See Berin Szoka & Adam Thierer, The Progress & Freedom Foundation, *Cyberbullying Legislation: Why Education is Preferable to Regulation*, , Progress on Point 16.2, June 19, 2009, www.pff.org/issues-pubs/pops/2009/pop16.12-cyberbullying-education-better-than-regulation.pdf; Adam Thierer, The Progress & Freedom Foundation, *Two Sensible, Education-Based Approaches to Online Child Safety*, Progress Snapshot 3.10, Sept. 2007, www.pff.org/issues-pubs/ps/2007/ps3.10safetyeducationbills.pdf.

⁴⁶ See Adam Thierer, The Progress & Freedom Foundation, *Congress, Content Regulation, and Child Protection: The Expanding Legislative Agenda*, Progress Snapshot 4.4, Feb. 6, 2008, www.pff.org/issues-pubs/ps/2008/ps4.4childprotection.html; Adam Thierer, The Progress & Freedom Foundation, *Is MySpace the Government's Space?*, Progress Snapshot 2.16, June 2006, www.pff.org/issues-pubs/ps/2006/ps_2.16_myspace.pdf

⁴⁷ See Berin Szoka & Adam Thierer, The Progress & Freedom Foundation, *COPPA 2.0: The New Battle over Privacy, Age Verification, Online Safety & Free Speech*, Progress on Point 16.11, May 2009, available at <http://pff.org/issues-pubs/pops/2009/pop16.11-COPPA-and-age-verification.pdf>; Adam Thierer, The Progress & Freedom Foundation, *Social Networking and Age Verification: Many Hard Questions; No Easy Solutions*, Progress on Point No. 14.5, Mar. 2007, www.pff.org/issues-pubs/pops/pop14.8ageverificationtranscript.pdf; Adam Thierer, The Progress & Freedom Foundation, *Statement Regarding the Internet Safety Technical Task Force's Final Report to the Attorneys General*, Jan. 14, 2008, www.pff.org/issues-pubs/other/090114ISTTFthiererclosingstatement.pdf; Nancy Willard, Center for Safe and Responsible Internet Use, *Why Age and Identity Verification Will Not Work—And is a Really Bad Idea*, Jan. 26, 2009, www.csriu.org/PDFs/digitalidnot.pdf; Jeff Schmidt, *Online Child Safety: A Security Professional's Take*, The Guardian, Spring 2007, www.jschmidt.org/AgeVerification/Gardian_JSchmidt.pdf.

⁴⁸ See Adam Thierer, The Progress & Freedom Foundation, *Closing the Book on COPA*, PFF Blog, Jan. 21, 2009, http://blog.pff.org/archives/2009/01/closing_the_book.html

Related PFF Publications

- *Cyberbullying Legislation: Why Education is Preferable to Regulation*, Berin Szoka & Adam Thierer, Progress on Point 16.2, June 19, 2009.
- *COPPA 2.0: The New Battle over Privacy, Age Verification, Online Safety & Free Speech*, Berin Szoka & Adam Thierer, Progress on Point 16.11, May 2009.
- *Parental Controls & Online Child Protection: A Survey of Tools and Methods*, Adam Thierer, Special Report, Version 3.1, Fall 2008.
- *Comments to the Federal Communications Commission in the Matter of Implementation of the Child Safe Viewing Act of 2007*, Adam Thierer, April 15, 2009.
- *Social Networking and Age Verification: Many Hard Questions; No Easy Solutions*, Adam Thierer, Progress on Point 14.5, March 21, 2007.
- *Social Networking Websites & Child Protection: Toward a Rational Dialogue*, Adam Thierer, Progress Snapshot 2.17, June 2006.
- *Cable's Commitment to Online Safety*, Adam Thierer, Progress Snapshot 3.7, June 2007.
- *Two Sensible, Education-Based Legislative Approaches to Online Child Safety*, Adam Thierer, Progress Snapshot 3.10 September 2007.
- *Rep. Bean's 'SAFER Net Act': An Education-Based Approach to Online Child Safety*, Adam Thierer, Progress on Point 14.3, Feb. 22, 2007.

The Progress & Freedom Foundation is a market-oriented think tank that studies the digital revolution and its implications for public policy. Its mission is to educate policymakers, opinion leaders and the public about issues associated with technological change, based on a philosophy of limited government, free markets and civil liberties. Established in 1993, PFF is a private, non-profit, non-partisan research organization supported by tax-deductible donations from corporations, foundations and individuals. The views expressed here are those of the authors, and do not necessarily represent the views of PFF, its Board of Directors, officers or staff.

The Progress & Freedom Foundation ■ 1444 Eye Street, NW ■ Suite 500 ■ Washington, DC 20005
202-289-8928 ■ mail@pff.org ■ www.pff.org