

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

DECEMBER 31, 2008



Berkman

The Berkman Center for Internet & Society
at Harvard University

ENHANCING CHILD SAFETY AND 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

December 31, 2008

Directed by the Berkman Center for Internet & Society at Harvard University

Chair: Professor John Palfrey

Co-Director: Dena T. Sacco

Co-Director and Chair, Research Advisory Board: danah boyd

Chair, Technology Advisory Board: Laura DeBonis

Coordinator: Jessica Tatlock

Task Force Members:

AOL/Bebo

Aristotle

AT&T

Berkman Center for Internet & Society at Harvard University (Directors)

Center for Democracy & Technology

Comcast

Community Connect Inc.

ConnectSafely.org

Enough Is Enough

Facebook

Family Online Safety Institute

Google Inc.

IAC

ikeepsafe

IDology, Inc.

Institute for Policy Innovation

Linden Lab

Loopt

Microsoft Corp

MTV Networks/Viacom.

MySpace and Fox Interactive Media

National Center for Missing & Exploited Children

The Progress & Freedom Foundation

Sentinel Tech Holding Corp.

Symantec

Verizon Communications, Inc.

Xanga

Yahoo!, Inc.

Wiredsafety.org

Executive Summary

Many youth in the United States have fully integrated the Internet into their daily lives. For them, the Internet is a positive and powerful space for socializing, learning, and engaging in public life. Along with the positive aspects of Internet use come risks to safety, including the dangers of sexual solicitation, online harassment, and bullying, and exposure to problematic and illegal content. The Multi-State Working Group on Social Networking, comprising 50 state Attorneys General, asked this Task Force to determine the extent to which today's technologies could help to address these online safety risks, with a primary focus on social network sites in the United States.

To answer this question, the Task Force brought together leaders from Internet service providers, social network sites, academia, education, child safety and public policy advocacy organizations, and technology development. The Task Force consulted extensively with leading researchers in the field of youth online safety and with technology experts, and sought input from the public. The Task Force has produced three primary documents: (1) a Literature Review of relevant research in the field of youth online safety in the United States, which documents what is known and what remains to be studied about the issue; (2) a report from its Technology Advisory Board, reviewing the 40 technologies submitted to the Task Force; and (3) this Final Report, which summarizes our work together, analyzes the previous documents as well as submissions by eight leading social network sites regarding their efforts to enhance safety for minors, and provides a series of recommendations for how to approach this issue going forward. Due to the nature of the Task Force, this Report is not a consensus document, and should be read in conjunction with the separate Statements from Task Force members included in the appendix.

At the outset, the Task Force recognized that we could not determine how technologies can help promote online safety for minors without first establishing a clear understanding of the actual risks that minors face, based on an examination of the most rigorously conducted research. The Task Force asked a Research Advisory Board comprising leading researchers in the field to conduct a comprehensive review of relevant work in the United States to date. The Literature Review shows that the risks minors face online are complex and multifaceted and are in most cases not significantly different than those they face offline, and that as they get older, minors themselves contribute to some of the problems. In broad terms, the research to date shows:

- Sexual predation on minors by adults, both online and offline, remains a concern. Sexual predation in all its forms, including when it involves statutory rape, is an abhorrent crime. Much of the research based on law-enforcement cases involving Internet-related child exploitation predated the rise of social networks. This research found that cases 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 notes that more research specifically needs to be done concerning the activities of sex offenders in social network sites and other online environments, and encourages law enforcement to work with researchers to make more data available for this purpose. Youth report sexual solicitation of minors by minors more frequently, but these incidents, too, are understudied, underreported to law enforcement, and not part of most conversations about online safety.
- Bullying and harassment, most often by peers, are the most frequent threats that minors face, both online and offline.

- The Internet increases the availability of harmful, problematic and illegal content, but does not always increase minors' exposure. Unwanted exposure to pornography does occur online, but those most likely to be exposed are those seeking it out, such as older male minors. Most research focuses on adult pornography and violent content, but there are also concerns about other content, including child pornography and the violent, pornographic, and other problematic content that youth themselves generate.
- 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. Social network sites are not the most common space for solicitation and unwanted exposure to problematic content, but are frequently used in peer-to-peer harassment, most likely because they are broadly adopted by minors and are used primarily to reinforce pre-existing social relations.
- Minors are not equally at risk online. Those who are most at risk often engage in risky behaviors and have difficulties in other parts of their lives. The psychosocial makeup of and family dynamics surrounding particular minors are better predictors of risk than the use of specific media or technologies.
- Although much is known about these issues, many areas still require further research. For example, too little is known about the interplay among risks and the role that minors themselves play in contributing to unsafe environments.

The Task Force asked a Technology Advisory Board (TAB) comprising technology experts from a range of backgrounds to solicit and review submissions from vendors and others offering currently available technologies. The TAB received 40 written submissions representing several categories of technologies, including age verification and identity authentication, filtering and auditing, text analysis, and biometrics. In sum, the TAB's review of the submitted technologies leaves the TAB in a state of cautious optimism, with many submissions showing substantial promise. The youth online safety industry is evolving. Many of the technologies reviewed were point solutions rather than broad attempts to address the safety of minors online as a whole. There is, however, a great deal of innovation in this arena as well as passionate commitment to finding workable, reasonable solutions from companies both large and small. The TAB emerged from its review process encouraged by the creativity and productivity apparent in this field.

The TAB and the Task Force note that almost all technologies submitted present privacy and security issues that should be weighed against any potential benefits. Additionally, because some technologies carry an economic cost and some require involvement by parents and teachers, relying on them may not protect society's most vulnerable minors.

The Task Force also asked all members from social network sites to provide overviews of their efforts to enhance safety for minors on their sites. These submissions reveal that much innovation – including the use of new technologies to promote safety for minors – is occurring at leading social network sites themselves. This innovation is promising and can be traced in no small part to the engagement of Attorneys General in this matter and the activities of the Task Force. As with the technology submissions, the steps being taken by the social network sites are helpful in mitigating some risks to minors online, but none is fail-safe.

The Task Force remains optimistic about the development of technologies to enhance protections for minors online and to support institutions and individuals involved in protecting minors, but cautions against overreliance on technology in isolation or on a single technological approach. Technology can play a helpful role, but there is no one technological solution or specific combination of technological solutions to the problem of online safety for minors. 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.

The Task Force does not believe that the Attorneys General should endorse any one technology or set of technologies to protect minors online. Instead, the Attorneys General should continue to work collaboratively with all stakeholders in pursuing a multifaceted approach to enhance safety for minors online. The Task Force makes specific recommendations in Part VII to the Internet community and to parents, as well as recommendations regarding the allocation of resources:

- Members of the Internet community should continue to work with child safety experts, technologists, public policy advocates, social services, and law enforcement to: develop and incorporate a range of technologies as part of their strategy to protect minors from harm online; set standards for using technologies and sharing data; identify and promote best practices on implementing technologies as they emerge and as online safety issues evolve; and put structures into place to measure effectiveness. Careful consideration should be given to what the data show about the actual risks to minors' safety online and how best to address them, to constitutional rights, and to privacy and security 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 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. Greater resources also should be allocated for ongoing research into the precise nature of online risks to minors, and how these risks shift over time and are (or are not) mitigated by interventions. To allow for more systematic and thorough research, law enforcement should work with researchers to help them gather data on registered sex offenders' use of Internet technologies and technology companies should provide researchers with appropriately anonymized data for studying their practices.
- Parents and caregivers should: educate themselves about the Internet and the ways in which their children use it, as well as about technology in general; explore and evaluate the effectiveness of available technological tools for their particular child and their family context, and adopt those tools as may be appropriate; be engaged and involved in their children's Internet use; be conscious of the common risks youth face to help their children understand and navigate the technologies; be attentive to at-risk minors in their community and in their children's peer group; and recognize when they need to seek help from others.