

**ARISTOTLE REBUTTAL TO FINAL REPORT OF THE
INTERNET SAFETY TECHNICAL TASK FORCE**

January 14, 2008

Executive Summary

Many youth in the United States have fully integrated the Internet into their daily lives. **[This report never gives a sense of what “many youth” means, because to do so would be to show the large numbers of youth that are affected by dangerous practices that the Report only addresses in terms of percentages of users. For example, MySpace reported that 1 in 4 Americans have a MySpace profile, and that 11% are under 18. This means that there are over 75M MySpace members in the US, with 8.5 M minors just on MySpace alone. Having these numbers provides context for how many actual kids the Report is talking about when referring to percentages in the research studies.]** 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. **[This completely misstates what the AGs asked the Task Force to do, which was to “find and develop online safety tools, with a focus on finding and developing online identity authentication tools primarily for social network sites in the United States. The Attorneys General also asked the Task Force to “establish specific and objective criteria that will be utilized to evaluate existing and new technology safety solutions”. Unfortunately, the Task Force acted primarily as self-appointed policy advisers, instead of answering the questions asked of the group as a technical task force.]**

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. **[Whose views are reflected in the Report? It is not a consensus document. Few votes were taken. The Report is unfocused and addresses far too many non-SNS, non-technical issues. Many recommendations are generic, obvious, and redundant. Preserving anonymity on SNS -- even for sex offenders - - appears to be an overriding principle.]**

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. **[This lone sentence appears calculated to excuse the Task Force for failing to focus on the issue of the conduct of Registered Sex Offenders on Social Network Sites. 50,000 registered sex offenders had been discovered on MySpace as of June 2008. This discovery was the seminal event behind formation of the Task Force Yet no studies have been done on this issue, and the data on the activities of these sex offenders on MySpace was never even requested for study by the Task Force at any time since formation, MySpace, of course, never offered this treasure trove of data on how RSOs operate so that the TF could study it. The fact that MySpace has this data on the activities of the 50000+ is not even mentioned in the Final Report. Worse, MySpace apparently continues to destroy this irreplaceable data without a word of objection in the Task Force Report. The failure of the Final Report to object to such destruction—and in fact to ignore it completely— is inexplicable and inexcusable. It represents a major failing of this Report.]** 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 Task Force, however, was expressly asked by the AGs to establish "specific and objective criteria that will be utilized to evaluate existing and new technology safety solutions." This objective was not met. Instead of establishing criteria as requested, the Report concludes that, "developing standard metrics for youth online safety solutions would be useful." In essence, we believe the Report is saying that someone else needs to do what the AGs asked the Task Force to do.]**

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. **[Again, the Report calls on law enforcement and technology companies to make data available. But the Report inexplicably ignores the fact that MySpace has data on the usage by at least 50,000 registered sex offenders, and instead of offering it for study, is destroying it. The Final Report should have stated clearly and unequivocally that current programs for**

destruction of such valuable and irreplaceable data before it has been studied must be suspended immediately.

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. To give families the tools they need, notice should be given to the user, and to the parent if known, the instant that a SNS has information that a child has even been contacted by an RSO. Such contacts should never, ever be presumed innocent. We have community notification in the real world whenever an RSO moves into the neighborhood. If there is good reason to sit on this information, such reason should have been included in the Report. The Final Report's complete silence on this issue – an issue raised repeatedly by Aristotle during the public and private Task Force meetings --is incomprehensible to us.

If there are laws that prevent an SNS from providing the Task Force with any information on the use of their site by RSOs (even in the aggregate), or from taking obvious steps to protect children (such as giving notice when an SNS learns that a RSO has contacted a minor child), this should have been addressed by the Task Force so that various options could be considered.]

I. Introduction

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. Minors use the Internet and other digital technologies to communicate with friends and peers, to connect with religious leaders and mentors, to conduct research for school assignments, to follow the progress of favorite sports teams or political candidates and participate in communities around shared interests, to read the news and find health information, to learn about colleges and the military, and in countless other productive ways. Most minors do not differentiate between their lives off and online, in part because the majority of online social interactions involving minors do not involve people who are not part of their offline lives.

Minors face risks online, just as they do in any other public space in which people congregate. These risks include harassment and bullying, sexual solicitation, and exposure to problematic and illegal content. These risks are not radically different in nature or scope than the risks minors have long faced offline **[This highly subjective characterization is directly contradicted by what follows in this paragraph about the entirely different nature and scope of risks offline and online]**, and minors who are most at risk in the offline world continue to be most at risk online. In the past, however, the risks were primarily local, and ideally addressed by parents, educators, social services, law enforcement and others working together at the local level. In the online context, the risks implicate services from companies and access to audiences from around the world. The technologies involved also make visible risky behaviors and problematic interactions that were less visible offline, while allowing at-risk youth to more publicly and prominently display signs that they need help. Parents and local community members often are unfamiliar with the relevant technologies and do not have direct experience with the way the risks evolve in the context of the Internet and interactive technologies. Addressing risks online therefore carries different challenges and requires broader collaboration to find innovative solutions.

The Internet Safety Technical Task Force was formed to consider, on an accelerated timeline, the extent to which technologies can play a role in enhancing safety for minors in these online spaces. **[As noted above, the Technical Task Force actually was asked to do something very specific: to “find and develop online safety tools, with a focus on finding and developing online identity authentication tools” primarily for social network sites in the United States. The Attorneys General also asked the Task Force to establish specific and objective criteria that will be utilized to evaluate existing and new technology safety solutions. An Internet-wide policy-oriented review -- such as that found in the Final report -- was simply not the task. The Task Force answered policy questions it was not asked, rather than providing the requested technical analysis.]** The Task Force was a collaborative effort among leaders from Internet service providers, social network sites, academia, education, child safety and public policy advocacy organizations, and technology development. The

Task Force was created in accordance with the Joint Statement on Key Principles of Social Networking Safety announced by the Attorneys General Multi-State Working Group on Social Network Sites and MySpace in January 2008, which is attached in Appendix A.

MySpace, in consultation with the Attorneys General, invited the members to participate in the Task Force. While all members brought different perspectives to the table, all were strongly committed to the common goal of enhancing protection for minors on the Internet. MySpace invited John Palfrey, Dena Sacco, and danah boyd – all from Harvard University’s Berkman Center for Internet & Society – to direct the Task Force. The Task Force held an organizational meeting in March 2008 and submitted this Final Report to the Attorneys General on December 31, 2008. The work we did during the intervening nine months is summarized in this Report.

This Report is being released at a time of dynamic change. The political, legislative, and economic context in which the Task Force began its work was markedly different from that at the conclusion. There has been a sea change in the political leadership of the country following the recent election of President-elect Obama. There is considerable speculation about the scope and reach of the proposed position of CTO for the United States, but this appointment and other campaign pledges appear very likely to have an impact on online safety going forward. In addition, a bill introduced by Senator Ted Stevens, the Protecting Children in the 21st Century Act, was incorporated into a larger broadband bill and recently signed into law by President Bush. This law calls upon the Department of Commerce’s National Telecommunications and Information Administration (the NTIA) to create a Working Group on a range of online safety issues, upon the FTC to develop national online safety awareness programs, and upon all schools that receive the e-rate to incorporate online safety education in curricula. The recently passed Pryor Bill instructs the FCC to review “advanced blocking technologies” to see whether there are ways to help parents better protect their children from inappropriate content in a converged media world. The FCC currently recently considered content filtering requirements as a condition for obtaining broadband spectrum in the upcoming AWS-3 auction. The Task Force is hopeful that our work will help to guide not only the important work of the Attorneys General with regard to online safety, but also the development and implementation of these and similar programs going forward.

II. Methodology

A. Development of a Project Plan

The Task Force began by reviewing past efforts in the area of youth online safety, including the work of the Child Online Protection Act (COPA) Commission (2000) and “Youth, Pornography, and the Internet” from the Computer Science and Telecommunications Board National Research Council (2002) in the United States, as well as related European efforts, such as the United Kingdom’s Byron Review entitled “Safer Children in a Digital World” (2008) and the European Commission’s

“Background Report on Cross Media Rating and Classification and Age Verification Solutions” (2008).

The Task Force used the findings of these related efforts as starting points to inform our work. As set forth in greater detail in the Project Plan attached in Appendix B, the scope of the Task Force’s inquiry was to consider those technologies that industry and end users – including parents – can use to help keep minors safer on the Internet. The Task Force identified the following three key questions:

1. Are there technologies that can limit harmful contact between children and other people?
2. Are there technologies that can limit the ability of children to access and produce inappropriate and/or illegal content online?
3. Are there technologies that can be used to empower parents to have more control over and information about the services their children use online?

Within each of these broad topic areas, the Task Force sought to identify the most pressing aspects of the problem and, in turn, which technologies are most likely to help companies, parents, children, and others in addressing those aspects.

The Task Force was chartered specifically with a focus on identity authentication tools and on social network sites in the United States. Although we focused on harms that occur in social network sites, the Task Force determined that we could not ignore the broader environment of the Internet as a whole, and that we would assess age verification technology in the context of other digital technologies that protect children online. Additionally, we placed emphasis on issues arising in the United States, but undertook to consider the problem of child safety on the Internet in an international context. The Task Force recognized from the outset that given limited time and resources and the dynamic nature of the issues, our work would represent a series of next steps, but not final answers, to these problems. Finally, although the Task Force’s focus was on technological solutions, we recognize that technology can work only in tandem with educational and law enforcement efforts.

As a note on terminology: throughout this report, the terms “youth,” “minors,” and “children” are used more or less interchangeably. There is a lack of uniformity in the use of such terms in public discourse and in the relevant scholarly literature. The Task Force has focused primarily on those young people who are under 18 years of age. The Task Force acknowledges that Internet safety issues are different for minors at various ages and developmental stages, and that any strategies should be targeted to subgroups of minors based on these and other factors, as discussed later in this Report.

B. Establishment of Advisory Boards

To assist in our work, the Task Force established two advisory boards: A Research Advisory Board (“RAB”) and a Technology Advisory Board (“TAB”). The

purpose of these supporting advisory boards was to enable us to accept input from experts on these topics who were not Task Force members (who were selected by MySpace at the outset of the Task Force process in early 2008).

The RAB was composed of leading researchers in the field. It provided information to the Task Force on what is known about the safety of minors online based on current research. It did so through a series of presentations to the Task Force, each of which was video-recorded and made available to the public on the Task Force's website, as well as through a comprehensive Literature Review of relevant research. A summary of the research is incorporated in Part III below, and the full Literature Review is attached in Appendix C. The Task Force intends for the Literature Review to help inform not only its own work, but also similar efforts going forward across the world.

The TAB was composed of technology experts, including academic computer scientists and computer forensics experts. It established a process for companies and individuals to submit to the Task Force information about technologies relevant to the protection of minors online. The TAB then reviewed those written submissions, answers to questions, and public presentations by some of the companies, and submitted a report to the Task Force regarding that review. A summary of the TAB's report is incorporated in Part IV below, and the full report is attached in Appendix D.

In addition, the Task Force asked members representing social network sites to provide information regarding the safety features they have in place to protect minors on their sites. Those submissions are described in Part V below and attached in Appendix E.

C. Task Force Meetings and Discussions

After our organizational meeting in March 2008, the full Task Force met four more times over the course of the year. At those meetings, the Task Force heard from the Research Advisory Board and other experts regarding current issues in youth online safety, heard from the Technology Advisory Board regarding its review of technology submissions, and worked on the contents of the project plan and the reports. Between meetings, the Task Force communicated frequently via email and our website.

In addition, in September 2008, the Task Force held a day-and-a-half public meeting at Harvard Law School in Cambridge, Massachusetts. The meeting was advertised on the Task Force's website, via press release, and by way of direct communication by Task Force members. Attorneys General Richard Blumenthal of Connecticut and Martha Coakley of Massachusetts addressed the public at the beginning of the meeting.

At this public meeting, Attorney General Blumenthal mentioned specifically that "MySpace has taken the initiative in eliminating about 50,000 child predators who have established profiles in their own names." The Task Force has taken note of and discussed this process in carrying out its work this year. This topic is a complex and important one. Figures of this sort do not appear in the research section of this report below because they have not been verified through a peer-reviewed research process.

[Although the 50,000 RSO figure doesn't appear in the research section supposedly because it was not verified through "peer-review", an example of the type of "peer-reviewed" study that the Task Force did rely on is discussed in endnote 1 at the conclusion of this document.¹ As shown in that endnote, it is almost inconceivable that the Final Report would rely on online surveys of 10-15 year to draw conclusions, while the discovery of 50,000 registered sex offenders identified through a match of government records and MySpace registrations is not deemed worthy of a single mention. The over-reliance of the Task Force on "peer-reviewed" studies -- no matter how little probative value they might have with respect to conduct on social network site – while completely ignoring real world data about tens of thousands of actual sex offenders, encapsulates the shortcomings of the Task Force report in a nutshell.] Researchers note that much remains to be asked and learned about this topic, and that it is important to learn more about who these Registered Sex Offenders are and what they do online in order to address concerns about their online activities.

The Task Force and members of the public then heard from some of the technology companies that submitted technologies for review, and learned more about others through a concurrent poster session. MySpace and Facebook addressed their own efforts in enhancing safety on their sites, and WiredSafety's teen Internet Safety experts, the TeenAngels, discussed their perspectives on the scope of the problem.

D. Quarterly and Final Reports

In addition to this Final Report, the Task Force submitted four quarterly reports to the Attorneys General. The Berkman team drafted the quarterly reports and the accompanying meeting minutes. All drafts were provided to the entire Task Force for comment before reports were finalized and shared with the Attorneys General and the public via the Task Force's website.

The Berkman Center team drafted this Final Report, with significant input from the Research and Technology Advisory Boards, each of which submitted their own documents to the Task Force. The draft of the Final Report then went to the entire Task Force. Members provided comments on the draft in two ways: (1) during a day-long discussion at the Task Force meeting on November 19, 2008; and (2) in writing before and after that meeting. The Task Force recognized at the outset that due to the diversity of our membership, we could not achieve unanimity on all of the findings and recommendations in this Report, and no formal vote was taken on its adoption. However, the Berkman Center team sought to incorporate comments whenever possible, and provided a revised draft to the entire Task Force to allow for an additional round of comments before finalizing the Report. In addition, all Task Force members were invited to submit separate Statements, which are attached in Appendix F. We urge all readers to consider these Statements in conjunction with this Report, the TAB's Report, and the Literature Review. Taken together, these documents give a sense of the extent to which the Task Force reached consensus.

E. Policy of Open Access to Information

Throughout the year, the Task Force sought to make our work as transparent as possible to the public. The Berkman Center established a public-facing website for the Task Force, accessible at <http://cyber.law.harvard.edu/research/isttf>. The Task Force also established a policy with regard to Intellectual Property, which is attached as Exhibit 3 to the TAB Report in Appendix D. Task Force documents were posted on the website, including the Project Plan, quarterly reports, meeting minutes, research from the RAB, the template for submissions to the TAB, and the submissions received by the TAB. The RAB presentations to the Task Force, as well as the entire public meeting in September 2008, were video-recorded, and those recordings were posted on the website. Harvard University will host and archive the website going forward.

III. Summary Report from the Research Advisory Board

A. Background

The Task Force's Research Advisory Board (RAB) was composed of scholars and researchers whose research addresses online safety for minors. The RAB was instructed to help the Task Force develop an understanding of what is currently known about safety issues with respect to minors and the Internet and, more specifically, social network sites.

Researchers and scholars from the United States whose work is relevant to the Task Force were invited to contribute through presentations and consultations. Researchers were invited to present their research to the Task Force based on the informative nature of their work and its relevance to the Task Force. Their presentations and a video of their talks are available on the Task Force's website. The RAB reached out to individuals with a record of ongoing, rigorous, and original research and invited them to directly participate in the creation of the Literature Review attached as Appendix C, by providing citations, critiques of the review, and otherwise expressing feedback. The RAB intended to be as inclusive as possible. Those who contributed to this process who wished to be identified are listed in Appendix C. The RAB also publicized a draft of the Literature Review for public and scholarly feedback and directly elicited responses from non-U.S. scholars working on this topic. Members of the research community who directly contributed to the RAB are:

- **Danah Boyd (Chair)**, University of California–Berkeley
- **David Finkelhor**, University of New Hampshire Crimes Against Children Research Center
- **Sameer Hinduja**, Florida Atlantic University
- **Amanda Lenhart**, Pew Internet and American Life Project [Presenter]
- **Sam McQuade**, Rochester Institute of Technology [Presenter]
- **Kimberly Mitchell**, University of New Hampshire Crimes Against Children Research Center
- **Justin Patchin**, University of Wisconsin–Eau Claire
- **Larry Rosen**, California State University at Dominguez Hills
- **Janis Wolak**, University of New Hampshire Crimes Against Children Research Center [Presenter]
- **Michele Ybarra**, Internet Solutions for Kids [Presenter]

B. Background to the Literature Review

The Literature Review attached in Appendix C is a review of original, published research addressing online sexual solicitation, online harassment and bullying, and exposure to problematic content. The bulk of this document was written by Andrew Schrock, the Assistant Director of the Annenberg Program in Online Communities at University of Southern California, and danah boyd, the Chair of the RAB and co-director of the Task Force. The purpose of this document is to provide a review of research in this area in order to further discussions about online safety. The RAB believes that to help youth in this new environment, the first step is to understand the actual threats that youth face and what puts them at risk. To do so, it is important to review the data. The RAB believes that the best solutions will be those that look beyond anecdotal reports of dangers and build their approaches around quantifiably understood risks and the forces that put youth at risk. The RAB also believes that solutions that are introduced should be measured as to their effectiveness in addressing the risks that youth actually face instead of measured in terms of adult perception at solving perceived risks.

Included in this review is methodologically sound research, with an emphasis on recent U.S.-focused, national, quantitative studies that addressed social media. Because the number of large-scale studies is limited, the review also includes smaller, regional studies and notes when a specific region is being discussed. Where appropriate, a limited number of older studies, qualitative findings, and studies outside of the United States are referenced for context. Studies commissioned by government agencies also are referenced, even when the sampling techniques are unknown and the findings were not vetted by peer review, because the RAB believed that work from these reputable organizations should be acknowledged. Reports and findings by other institutions were handled more cautiously, especially when the RAB was unable to vet the methodological techniques or when samples reflected problematic biases. The RAB did not exclude any study on the basis of findings, nor did it exclude any peer-reviewed study on the basis of methodology. In choosing what to review, the RAB was attentive to methodological rigor, because it wanted to make sure that the Task Force had the best data available.

The methodology of a study is its most important quality. The size of a sample population matters less than how the population was sampled in relation to the questions being asked. The questions that qualitative studies can address differ from those that can be addressed quantitatively, but both are equally valid and important. For most of the concerns brought forth by the Task Force, the RAB thought it was important to focus on those questions best addressed through quantitative means.

Presenting statistical findings is difficult, because those who are unfamiliar with quantitative methodology may misinterpret the data and read more deeply into the claims than the data supports. For example, correlation is not the same as causation, and when two variables are correlated, the data cannot tell you whether one causes the other or whether an additional mediating variable that affects both is involved. In presenting the findings of different studies, the Literature Review tries also to provide a roadmap for understanding what these studies mean and also includes some background on methodology for those who want a better overview of the topic.

Although numerous studies are currently underway and much research is available to address online safety concerns, very few of the findings enter public or political discourse. This is unfortunate, because the actual threats that youth may face appear to be different than the threats most people imagine. More problematically, media coverage has regularly mischaracterized research in this area, thus contributing to inaccurate perceptions of what risks youth face. This problem was most visible in the public coverage of the Online Victimization studies done at the Crimes Against Children's Research Center (Finkelhor et al. 2000; Wolak et al. 2006). These reports are frequently referenced to highlight that one in five or one in seven minors are sexually solicited online. Without context, this citation implies massive solicitation of minors by older adults. As discussed below, other peers and young adults account for 90%-94% of solicitations in which approximate age is known (Finkelhor et al. 2000; Wolak et al. 2006). Also, many acts of solicitation online are harassing or teasing communications that are not designed to seduce youth into offline sexual encounters; 69% of solicitations

involve no attempt at offline contact (Wolak et al. 2006). Misperception of these findings perpetuates myths that distract the public from solving the actual problems youth face.

This summary highlights some of the major findings from key studies to provide an overview of the full document. The statistics presented here are better read in context, but are used here to offer a sense of scale. It also provides a descriptive overview of what the studies presented in the review mean. This is not a substitute for the data; those who want more depth or who plan to apply the statistics presented should read the full Literature Review and the original research cited therein.

This summary also points out the weaknesses of some of the current studies and the need for more research. This is a dynamic space and it is important that studies are ongoing, tracking changes as the environment changes. It is clear that more research is necessary to understand the behaviors and profile of adult offenders. It is also clear that studies on online harassment suffer from inconsistent definitions and that too little is known about certain types of problematic content. That said, except with respect to the definitions of bullying, the research presented is fairly consistent across studies with different populations, affirming the fundamental question of validity.

Finally, some Task Force members have expressed a concern that because the time involved in collecting data, interpreting results, and publishing studies is often long, the findings presented here are irrelevant to current debates and usage. This view is reasonable, but also inaccurate. The research presented here shows clear trends over time and across different genres of social media **[but not with respect to solicitation on Social networks and therefore its relevance to the purpose of this Task Force is highly suspect]** and age ranges; also, the research is frequently affirmed by multiple studies. There is also clear indication that psychosocial problems and risky behaviors are the dominant factors correlated with risk across all genres of social media.

To further assuage doubt, the RAB contacted all of the scholars working on national studies and asked them to review the data that they are currently analyzing for any salient shifts. Based on their preliminary analysis of data from upcoming studies, there are no major departures from current trends in the near future.

C. Summary of Literature Review

The rapid rise of social network sites and other genres of social media among youth is driven by the ways in which these tools provide youth with a powerful space for socializing, learning, and participating in public life (boyd 2008; Ito et al. 2008; Palfrey and Gasser 2008). The majority (59%) of parents say the Internet is a “positive influence” in their children’s lives (Rideout 2007), but many have grave concerns about the dangers posed by the Internet. Contemporary fears over social network sites resemble those of earlier Internet technologies, but – more notably – they also seem to parallel the fears of unmediated public spaces that emerged in the 1980s that resulted in children losing many rights to roam (Valentine 2004). There is some concern that the mainstream media amplifies these fears, rendering them disproportionate to the risks youth face. This

creates a danger that known risks will be obscured, and reduces the likelihood that society will address the factors that lead to known risks, and often inadvertently harm youth in unexpected ways.

This is not to say that there are no risks, but that it is important to ask critical questions in order to get an accurate picture of the online environment and the risks youth face there. The Literature Review attached in Appendix C summarizes ongoing scholarly research that addresses these questions:

1. What threats do youth face when going online?
2. Where and when are youth most at risk?
3. Which youth are at risk and what makes some youth more at risk than others?
4. How are different threats interrelated?

The findings of these studies and the answers to these questions are organized around three sets of online threats: *sexual solicitation*, *online harassment*, and *problematic content*. Two additional sections focus on what factors are most correlated with risk and the role of specific genres of social media. There is also documentation of child pornography as it relates to youth's risks and a discussion of understudied topics and directions for future research. This overview summarizes the key findings presented in the review alongside a descriptive roadmap that provides context. It is not meant as a substitute for reading the full Literature Review.

1. Sexual Solicitation and Internet-Initiated Offline Encounters

Although numerous studies have examined sexual solicitation, three national datasets provide the most statistically valid findings – N-JOV, YISS-1, and YISS-2 – and are regularly analyzed in articles by Wolak, Finkelhor, Ybarra, and Mitchell. Findings in regional studies (e.g., McQuade and Sampat 2008; Rosen et al. 2008) affirm their trends. **[Again, these studies do not address the behavior of tens of thousands of registered sex offenders and millions of minors social network sites, where large amounts of personal data are posted, and interaction between minors and adults is the norm.]**

The percentages of youth who receive sexual solicitations online have declined from 19% in 2000 to 13% in 2006 and most recipients (81%) are between 14–17 years of age (Finkelhor et al. 2000; Wolak et al. 2006). For comparison, a regional study in Los Angeles found that 14% of teens reported receiving unwanted messages with sexual innuendos or links on MySpace (Rosen et al. 2008) and a study in upstate New York found that 2% of fourth through sixth graders were asked about their bodies, and 11% of seventh through ninth graders and 23% of tenth through twelfth graders have been asked sexual questions online (McQuade and Sampat 2008). The latter study also found that 3% of the older two age groups admitted to asking others for sexual content (McQuade and Sampat 2008).

Youth identify most sexual solicitors as being other adolescents (48%; 43%) or young adults between the ages of 18 and 21 (20%; 30%), with few (only 4%; 9%) coming from older adults and the remaining being of unknown age (Finkelhor et al. 2000; Wolak et al. 2006). Not all solicitations are from strangers; 14% come from offline friends and acquaintances (Wolak et al. 2006, 2008b). Youth typically ignore or deflect solicitations without experiencing distress (Wolak et al. 2006); 92% of the responses amongst Los Angeles–based youth to these incidents were deemed “appropriate” (Rosen et al. 2008). Of those who have been solicited, 2% have received aggressive and distressing solicitations (Wolak et al. 2006). Though solicitations themselves are reason for concern, few solicitations result in offline contact. Social network sites do not appear to have increased the overall risk of solicitation (Wolak et al. 2008b); chat rooms and instant messaging are still the dominant place where solicitations occur (77%) (Wolak et al. 2006).

A study of criminal cases in which adult sex offenders were arrested after meeting young victims online found that victims were adolescents and few (5%) were deceived by offenders claiming to be teens or lying about their sexual intentions; 73% of youth who met an offender in person did so more than once (Wolak et al. 2008b). Although identity deception may occur online, it does not appear to play a large role in criminal cases in which adult sex offenders have been arrested for sex crimes in which they met victims online. Interviews with police indicate that most victims are underage adolescents who know they are going to meet adults for sexual encounters and the offenses tended to fit a model of statutory rape involving a post-pubescent minor having nonforcible sexual relations with an adult, most frequently adults in their twenties (Wolak et al. 2008a). Hines and Finkelhor note that youth often initiate contact and sexual dialogue; they are concerned that “if some young people are initiating sexual activities with adults they meet on the Internet, we cannot be effective if we assume that all such relationships start with a predatory or criminally inclined adult” (Hines and Finkelhor 2007: 301).

Not all youth are equally at risk. 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). Patterns of risky behavior are also correlated with sexual solicitation and the most significant factor in an online connection resulting in an offline sexual encounter is the discussion of sex (Wolak et al. 2008b). Youth 15–17 years old are at the greatest risk, because they tend to engage in the riskiest behavior, and are most likely to communicate with strangers online (Wolak et al. 2008b).

Sexual solicitation and predation are serious concerns, but the image presented by the media of an older male deceiving and preying on a young child does not paint an accurate picture of the nature of the majority of sexual solicitations and Internet-initiated offline encounters; this inaccuracy leads to major risks in this area being ignored. Of particular concern are the sexual solicitations between minors and the frequency with which online-initiated sexual contact resembles statutory rape rather than other models of abuse. Finally, though some technologies can be more easily leveraged than others for

solicitation, risk appears to be more correlated with a youth's psychosocial profile and risky behaviors than any particular technological platform.

2. Online Harassment and Cyberbullying

It is difficult to measure online harassment and cyberbullying, because these concepts have no clear and consistent definition. Some definitions include acts that embarrass or humiliate youth while others include only those that are deemed threatening. As a result, the frequency with which youth report being victimized varies wildly between studies (4%–46%) (Hinduja and Patchin 2009; Kowalski et al. 2007; Lenhart 2007; McQuade and Sampat 2008; Smith et al. 2008; Williams and Guerra 2007; Wolak et al. 2006; Ybarra et al. 2007a). Although each study is internally consistent and methodologically sound, an outsider might argue over whether the incidents being measured do or do not constitute harassment or bullying, making it difficult to translate these numbers into holistic impressions of the state of harassment and bullying. Furthermore, without consistent definitions across scholars, it is difficult to compare the studies. For all of these caveats, what is known is that using most definitions, online harassment or cyberbullying happens to a significant minority of youth, is sometimes distressing, and is frequently correlated with other risky behaviors and disconcerting psychosocial problems (Patchin and Hinduja 2006; Ybarra and Mitchell 2007), just as is the case offline (Hawker and Boulton 2000). Ybarra and Wolak (2007) found that 39% of victims reported emotional distress over being harassed online, that both victims and perpetrators are significantly more likely to use substances and experience depressive symptomatology, and that online victims are significantly more likely to harass others online and be victims of offline bullying.

Studies consistently find that youth reports of that bullying are more common than online harassment (Lenhart 2007; Li 2007; Smith et al. 2008; Williams and Guerra 2007), but this does not diminish the costs of online harassment. Hinduja and Patchin (2009) also found that 42.4% of youth who report being cyberbullied also report being bullied at school. Offline, adults are frequently unaware that bullying is taking place – let alone present at the moments in which it occurs. Online harassment may be more public and leaves traces that adults can later view (boyd 2008).

In online contexts, perpetrators may appear to be anonymous, but this does not mean that the victims do not know the perpetrators or that the victims are not able to figure out who is harassing them. Wolak et al. (2006) found that 44% know the perpetrator offline, but Hinduja and Patchin (2009) found that 82% know their perpetrator (and that 41% of all perpetrators were friends or former friends). Hinduja and Patchin suggest that the difference between their data may be a result of shifts in the practice of online harassment. Sibling-based online harassment is also reported, but not well measured; one regional study in New York found that 30.5% of seventh through ninth graders who reported being victimized online in some way (not just harassment) indicated that a nonparent family member was the perpetrator (McQuade and Sampat 2008). All studies reported that other youth constituted almost all of known cyberbullies. Studies differ on whether or not there is a connection between online and offline bully perpetration and victimization (Hinduja and Patchin 2007; Kowalski and Limber 2007; Raskauskas and Stoltz 2007; Ybarra et al. 2007a), but there is likely a partial overlap.

Likewise, the data vary on the overlap between bullies and victims (Beran and Li 2007; Kowalski and Limber 2007; Ybarra and Mitchell 2004a); a recent study found that 27% of teenaged girls were found to “cyberbully back” in retaliation for being bullied online (Burgess-Proctor et al. 2009).

Offline bullying tends to peak in middle school (Devoe et al. 2005), but online harassment tends to peak later and continue into high school (Smith et al. 2008; Wolak et al. 2006). Reports of gender differences are inconclusive, but generally, girls appear more likely to be online harassment victims (Agatston et al. 2007; DeHue et al. 2008). Although there are high-profile examples of adults bullying minors, it is not clear how common this is. Wolak et al. (2006) found that 73% of known perpetrators were other minors, but it is not clear how many of the remaining who are eighteen and over were young adults or slightly older peers. Other studies suggest that minors are almost exclusively harassed by people of similar age (Hinduja and Patchin 2009).

It is difficult to pinpoint the exact prevalence of cyberbullying and online harassment, because the definitions themselves vary, but the research is clear that this risk is the most common risk minors face online. Though there is a strong correlation between victimization (and perpetration) and psychosocial problems, causality is unknown. In other words, stopping online harassment may not curb the psychosocial problems that these minors face and addressing the psychosocial problems may be necessary to reduce incidents of online harassment. In order to help the most minors, addressing online harassment and its underlying causes should be the top priority.

3. Exposure to Problematic Content

Problematic Internet-based content that concerns parents covers a broad spectrum, but most research focuses on violent media (movies, music, and images) and adult pornography. Other problematic content that emerges in research includes hate speech, content discussing or depicting self-harm, child pornography, and content that could be considered obscene. Depending on one’s family values, more categories of content may be considered problematic, but research has yet to address these other issues.

There are three core concerns with respect to problematic content: (1) youth are unwittingly exposed to unwanted problematic content during otherwise innocuous activities; (2) minors are able to seek out and access content to which they are forbidden, either by parents or law; (3) the intentional or unintentional exposure to content may have negative psychological or behavioral effects on children. The Literature Review focuses on the first two issues.

Encounters with pornography are not universal and rates of exposure are heavily debated. In a recent national study, 42% of youth reported either unwanted or wanted exposure or both; of these, 66% reported only unwanted exposure, and 9% of those indicated being “very or extremely upset” (Wolak et al. 2006). Rates of unwanted exposure were higher among youth who were older, reported being harassed or solicited online, victimized offline, and were depressed (Wolak et al. 2007). Most studies found

that males and older adolescents are more likely to be exposed to pornography (Flood 2007; Sabina et al. 2008; Ybarra and Mitchell 2005), but younger children are more likely to be distressed by it (Wolak et al. 2006).

While use of the Internet is assumed to increase the likelihood of unwanted exposure to pornography, this may not be true among all demographics. Younger children report encountering pornographic content offline more frequently than online (10.8% versus 8.1%) (Ybarra and Mitchell 2005) and a study of seventh and eighth graders found that of those who are exposed to nudity (intentionally or not), more are exposed through TV (63%) and movies (46%) than on the Internet (35%) (Pardun et al. 2005).

This finding, repeated across multiple studies with different methodologies and populations, raises more questions than it answers, especially because it conflicts with commonly held assumptions. Is exposure to pornography dependent on what kinds of Internet access these youth have (home access vs. school access)? Would the data look different if nudity were classified differently or broken down? Are certain types of households more likely to expose children to R- or X-rated TV shows and movies? Are families more likely to filter Internet content than TV and movie content? More qualitative research is necessary to uncover why younger children report being exposed to more pornographic content in traditional media than new media, but these findings do suggest that a high level of availability does not always equal exposure.

Exposure to violent content presents different concerns, because it usually occurs as a part of common online activities – children are exposed to violent content through videogames, on news sites, and through videos that are circulated among youth. Studies in the UK found that 31% of youth reported seeing violent content online (Livingstone and Bober 2004), but there are no studies that properly assess the frequency of exposure to violent content in the United States.

At present, the majority of research on problematic content focuses on exposure and consumption, although there are indications that youth are also contributing to the production of problematic content. Youth-created or -distributed problematic content includes fight videos, hate speech, pornographic images or videos of oneself or one's friends, and content for pro-eating disorder and self-injury websites. At present, there is limited data about the frequency of youth-generated problematic content or the psychosocial characteristics of those youth who contribute to it.

4. Different Risks

With all three types of threats (sexual solicitation, online harassment, and problematic content), some minors are more likely to be at risk than others. Generally speaking, the characteristics of youth who report online victimization are similar to those of youth reporting offline victimization and those who are vulnerable in one online context are often vulnerable in multiple contexts (Finkelhor 2008). In the same way, those identified as “high risk” (i.e., experienced sexual abuse, physical abuse, or parental

conflict) were twice as likely to receive online solicitations (Mitchell et al. 2008) and a variety of psychosocial factors (such as substance use, sexual aggression, and poor bonds with caregivers) were correlated with online victimization (Ybarra et al. 2007b, 2007c).

Depression, abuse, and substances are all strongly correlated with various risky behaviors that lead to poor choices with respect to online activities. A poor home environment that includes conflict and poor parent–child relationships is correlated with a host of online risks (Wolak et al. 2003; Ybarra and Mitchell 2004b).

Talking with strangers online does not appear to be universally risky, but it may increase the possibility of sexual solicitation, particularly among youth who are willing to engage in conversations about sexual topics (Wolak et al. 2008a). With talking to strangers, it is difficult to discern cause and effect – are youth more at risk because they talk to strangers or are at-risk youth more likely to talk to strangers?

Making connections online that lead to offline contact is not inherently dangerous. A regional study in New York found that 10% of seventh through eighth graders and 14% of tenth through twelfth graders have invited people they met online to meet offline (McQuade and Sampat 2008). **[The description of this statistic has been massaged to soften its potential impact. The task force was told by Dr. McQuade that these large percentages of young students have invited, or accepted invitations from, online “strangers” to meet offline. Given how many students use social network sites, the number of minors who are agreeing to offline encounters with complete online strangers is shockingly and disturbingly high. To put this in perspective, if MySpace has 8.5 million minors, and 10%-14% are agreeing to meet online strangers offline, this means more than a million minors are engaged in such conduct. This should alarm any parent who hears it.]** An early study **[done before the popularity of social network sites exploded]** found that Internet-initiated connections resulting in offline contact are typically friendship-related, nonsexual, formed between similar-aged youth, and known to parents (Wolak et al. 2002); recent qualitative studies find similar patterns (Ito et al. 2008). For socially ostracized youth, these online connections may play a critical role in identity and emotional development (Hiller and Harrison 2007).

Contrary to popular assumptions, posting personally identifying information does not appear to increase risk in and of itself. Rather, risk is associated with interactive behavior. Further, youth who engage in a high number of different potentially risky online behaviors (e.g., having unknown people on a buddy list, seeking pornography online, using the Internet to harass others) are also more at risk (Wolak et al. 2008b; Ybarra et al. 2007c).

Though many of the studies focus on the Internet at large, minors face different risks in different online environments, sometimes because technologies facilitate certain kinds of communication between adults and minors or among minors. For instance, on social network sites, a popular genre of social media among youth, teens are more likely

to interact with friends or friends-of-friends than complete strangers (Lenhart and Madden 2007). Norms may also play a role. For example, in gaming communities, it is more normative for youth to interact with people they do not know. At-risk youth are more attracted to some environments, such as sexually oriented chat rooms, thus elevating their levels of risk, as is demonstrated when depressed or sexually promiscuous youth are more frequent users of online chat and forums. Finally, certain environments provide means to actively combat solicitation and harassment, such as by blocking or ignoring users.

Although there is a correlation between online risk and high levels of online participation, online participation does not predict risk. Youth who are solicited and harassed do indicate that all genres of social media (IM, chat rooms, social network sites, email, blogging) are their top online activities (Ybarra and Mitchell 2008).

The risks presented by social network sites – most notably with respect to solicitation and, to a lesser degree, harassment – appear to be consistent with Internet risks more broadly and lower than those in other media (Ybarra and Mitchell 2008). **[See discussion of Ybarra and Mitchell 2008 in endnote 1. On the question of whether social network sites such as MySpace increase the risk of victimization by online molesters, the leading researchers state that although conclusions drawn from the small amount of relevant research available suggest that fears about SNS have been overstated, “caution should be used in interpreting this small amount of research about a new phenomenon” (Wolak et al. 2008b). For the Report to leave out such an important disclaimer demonstrates a lack of balance and the promotion of an agenda that has nothing to do with the analysis of technology that the Task Force was asked to perform.]** Studies with broader definitions of bullying suggest that social network sites present an equal or slightly increased risk (Lenhart 2007), in part because these sites are popular tools of peer communication.

5. Future Research

In addition to the topics discussed here, some areas of youth online safety are critically under-researched, particularly: (1) minor–minor solicitation; (2) the creation of problematic (sexual, violent, self-harm) content by minors; (3) less visible groups, such as gay, lesbian, bisexual, or transgender (LBGT) youth and youth with disabilities who may be particularly vulnerable; (4) the interplay between socioeconomic class and risk factors; (5) the role that pervasive digital image and video capture devices play in minor-to-minor harassment and youth production of problematic content; (6) the intersection of different mobile and Internet-based technologies; and (7) the online activities of registered sex offenders. New research in this area requires a combination of funding and access. For example, researching the online activities of registered sex offenders requires the support and engagement of law enforcement and technology companies.

New methodologies and standardized measures that can be compared across populations and studies are also needed to illuminate these under-researched topics.

Finally, because new environments present new risks, there is a need for ongoing large-scale national surveys to synchronously track these complex dynamics as they unfold.

IV. Summary Report from the Technology Advisory Board

In parallel to the work of the RAB, the TAB solicited, evaluated, and reviewed 40 written public submissions of technologies, and drew conclusions from these submissions about the state of technologies intended to enhance online safety for minors in a formal process described in detail in the report in Appendix D. The primary task of the TAB was to assess whether and how the submitted technologies would be useful in the context of enhancing online safety for minors. To conduct its work, the TAB was limited to the submission itself, written responses to several questions, and public presentations made to the Task Force. The TAB did not perform uniform, independent technical evaluations of the technologies submitted.

The technology categories that the TAB assigned, with the number of submissions in parentheses, were:

1. Age Verification/Identity Authentication (17)
2. Filtering/Auditing (13)
3. Text Analysis (5)
4. Biometrics (1) (+2 with biometrics as secondary category)
5. Other (4)

The objective criteria that the TAB used in assessing the technology take the form of 14 evaluative questions, which are included in the TAB Report in Appendix D.

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.

By the end of the review process, the TAB determined that no single technology reviewed could solve every aspect of online safety for minors, or even one aspect of it one hundred percent of the time. At the same time, there is clearly a role for technology in addressing this issue both now and in the future; most likely, various technologies should be leveraged together to help address the challenges in this arena.

Some critics may object to the use of technology as a solution, given the risk of failure and lack of total certainty around performance. However, the TAB believes that, though it is indeed true that even the cleverest, most robust technology can be circumvented, this does not necessarily mean that technology should not be deployed at all. It simply means that – even with deployment of the best tools and technologies

available to jumpstart the process of enhancing safety for minors online – there is no substitute for a parent, caregiver, or other responsible adult actively guiding and supporting a child in safe Internet usage. Even the best technology or technologies should be only part of a broader solution to keeping minors safer online.

As a corollary, the TAB recommends that further evaluative work be conducted on any technology – whether or not it was among those reviewed in this process – prior to endorsing or broadly recommending its use, given the potential for significant new risks and unintended consequences. The benefits of each solution reviewed need further exploration and balancing against monetary costs, possible privacy and security concerns about user information, international implications and applicability, as well as other issues. Additionally, determining which technology or set of technologies will work best for a particular child, family, school, community, or any other context in which the safety of minors on the Internet is an immediate concern will always be a highly individualized decision. It is not always a decision that can reasonably be made without a great deal of familiarity with the situation in which a technology solution would function.

Listed here, and discussed in greater detail in the full TAB Report in Appendix D, are the specific conclusions and recommendations generated by the TAB’s review process:

- Technology can play a role but should not be the sole input to improved safety for minors online.
- The most effective technology solution is likely a combination of technologies.
- Any and every technology solution has its limitations.
- Youth online safety measures must be balanced against concerns for the privacy and security of user information, especially information on minors.
- For maximum impact, client-side-focused technologies should be priced to enable all would-be users to purchase and deploy them.
- A common standard for sharing information among safety technologies would be useful.
- Developing standard metrics for youth online safety solutions would be useful. [We believe that these should have been the “specific and objective criteria that will be utilized to evaluate existing and new technology safety solutions”, as requested by the AGs.]

The Members of the TAB were:

- **Ben Adida**, Harvard Medical School, Harvard University

- **Scott Bradner**, Harvard University
- **Laura DeBonis**, Berkman Center, Harvard University (chair)
- **Hany Farid**, Dartmouth College
- **Lee Hollaar**, University of Utah
- **Todd Inskip**, Bank of America
- **Brian Levine**, University of Massachusetts–Amherst
- **Adi Mcabian**, Twistbox
- **RL Morgan**, University of Washington
- **Lam Nguyen**, Stroz Friedberg, LLC
- **Jeff Schiller**, Massachusetts Institute of Technology
- **Danny Weitzner**, Massachusetts Institute of Technology

Observers to the TAB were:

- **Rachna Dhamija**, Usable Security Systems
- **Evie Kintzer**, WGBH
- **Al Marcella**, Webster University
- **John Morris**, Center for Democracy and Technology
- **Teresa Piliouras**, Polytechnic University
- **Greg Rattray**, Delta-Risk
- **Jeff Schmidt**, Consultant
- **John Shehan**, National Center for Missing and Exploited Children

The full report of the TAB is attached to this Report in Appendix D.

V. Overview of Online Safety Efforts Made by Social Network Sites

In part through this Task Force process and as a result of the efforts of Attorneys General in bringing attention to the issue of youth online safety, social network sites have themselves continued to make strides in enhancing safety features on their sites to protect minors. The Task Force asked all Task Force representatives from social network sites to submit an overview of their efforts to enhance safety for minors on their sites. In response, the Task Force received eight submissions from social network sites, all of which are attached in Appendix E. These submissions were made by Bebo and AOL, Community Connect Inc., Facebook, Google orkut, Loopt, MySpace, MTV Networks/Viacom, and Yahoo!. These submissions were not reviewed by the TAB.

All of these companies develop and adopt technologies to protect children. The technologies they develop in-house are designed around their particular features, the users on their sites, and the issues that arise. All are committed to ongoing improvements in this area. The Task Force summarizes the following efforts of these eight leading social network sites, all taken from the submissions attached in Appendix E:

- **Report Abuse:** All eight of the social network sites who submitted to the Task Force provide a technology-driven mechanism by which users can report abuse to the site's operators.
- **Access to Age-Appropriate Content:** Several of the eight social network sites who submitted to the Task Force restrict users registered as minors from accessing certain inappropriate content. For example: AOL has online services for minors with age-appropriate content; Community Connect Inc. does not show minors advertisements designed for adults; MySpace denies users under 18 access to certain age-inappropriate areas, does not allow them to browse for certain inappropriate categories, and blocks access to advertisements related to alcohol, smoking, and drinking; and Yahoo! has search features designed specifically for minors that prevent the display of adult content.
- **Parental Control Software:** Some of the eight social network sites who submitted to the Task Force provide parental controls. For example, AOL and MySpace offer parental control software to their users for use in conjunction with their sites. Yahoo! offers parental controls via its access partners, such as AT&T and Verizon. Community Connect Inc.'s "Safety Tips for Parents includes a suggestion to consider using computer based blocking software."
- **Review for Inappropriate and Illegal Content:** Most of the eight social network sites who submitted to the Task Force review to some degree their own online spaces for inappropriate and illegal content, including pornography and child pornography, in addition to responding to user reports regarding such content. AOL, for instance, "has implemented technologies to identify and remove images of child pornography and to help eliminate the sending of known child pornography," including blocking transmissions of "apparent pornographic images." In addition, Bebo "proactively seeks out inappropriate content using software and other mechanisms to review such content"; Community Connect Inc. uses a "photo approval process for all social main photos to prevent inappropriate photos from appearing as the main photo on personal pages" and requires approval for "all main photos in Groups"; Facebook deploys a variety of technology tools, including easily available reporting links on photos and videos; Google orkut employs "image scanning technology" to detect child pornography and pornography; Yahoo! has "implemented technologies and policies" to help identify apparent child pornography violations on its network; MTV Networks/Viacom screens uploads for inappropriate content using "human moderation and/or identity technologies"; and MySpace "reviews images and videos that are uploaded to the MySpace servers and photos deep-linked from third-party sites."
- **Peer Verification for Minors:** Facebook uses a peer verification system for users who identify themselves as under 18. MySpace has a closed school section that relies on peer approval and moderation to separate current students from alumni

and provides a report abuse category that allows current users to report underage users.

- **Restrictions on Changing Age Information after Registration:** Some of the eight social network sites who submitted to the Task Force restrict users from changing their date of birth or age after they have registered. For example, MySpace offers alerts, via its ParentCare software, to parents whose children change their ages and controls that limit how minors may change their ages. On Facebook, users cannot edit their birth date to one that makes them under 18 without first contacting the “User Operations Team for review.” On Community Connect, Inc., “members can not change their date of birth after registering.”
- **Enforcement of Age Restrictions:** Several of the eight social network sites who submitted to the Task Force use cookies or other technology to help enforce age restrictions. For example: Community Connect Inc. places a cookie on a registrant’s browser to help prevent age falsification; people who try to sign up on Facebook with a birth date that makes them under 13 are blocked, and a persistent browser cookie is used to prevent further attempts at signing up; Google places a session cookie on a registrant’s browser to help prevent age falsification when a user registers for orkut; and MySpace places a cookie on a registrant’s browser to help prevent age falsification in addition to employing an algorithm to locate and remove underage users. Loopt has implemented an “age-neutral” screening mechanism in its subscriber registration flow, which requires users to input their age, blocks users who do not meet the minimum requirement, and tags the mobile device of such unsuccessful registrants and prevents reregistration from the same device.
- **Restrictions on Searching for Minors:** Several of the eight social network sites who submitted to the Task Force restrict the ability of users registered as adults from searching for users registered as minors. For example: Bebo does not allow the use of search engines to search for users under 16; Facebook does not allow minors and adults on the same regional network to see one another’s profiles and does not allow adults to search for minors based on profile attributes; MTV Networks/Viacom does not allow adults to search for minors, and adults can become “friends” with users under 16 only if they know the user’s last name, email address, or username; and on MySpace, profiles for users under 18 are set to “private” upon account creation by default, and adults cannot add a user under 16 as a friend without knowing that user’s last name or email address.
- **Removal of Registered Sex Offenders:** MySpace [has identified this as one of the “The ‘Big Six’ Basics for Online Safety” and] uses one of the technologies submitted to the Task Force to identify and remove registered sex offenders from its site [This statement glosses over a critical point. To the extent the technology is effective, it is only to identify and remove offenders who have registered using their real identities. It is self-evident that RSOs cannot be identified/removed if allowed to

register with false data. As the Kentucky AG stated, "They swept over 50,000 registered sex offenders off of MySpace and ladies and gentlemen we're catching the dumb ones. We're catching the ones using their registered sex offender email to get on MySpace."ⁱⁱⁱ We cannot know how many more RSOs are registered under false credentials, beyond the confirmed 50,000 (as of June 2008). Identity authentication complements RSO Removal, and shores up this obvious weakness in that process, by providing more confidence that registrants are who they say they are. Otherwise, the RSO Removal process may actually increase the risks to minors by creating a false sense of security, when in truth the process is catching only the "dumb" RSOs. MySpace has never provided the Task Force with information to be able to evaluate the effectiveness of this technology, so that we can answer questions such as whether there is evidence that RSOs are re-registering under false IDs after being identified as RSOs and having their profiles removed; or whether RSOs are simply giving up on MySpace and going elsewhere after being flagged and removed.]

- Facebook disables the accounts of convicted sex offenders and plans to "add the KidsAct registry" to disable accounts and prevent those on the list from registering. MTV Networks/Viacom is "exploring utilizing sex offender registry software to assist us in locating and removing RSO's" from its sites.
- **Amber Alerts:** AOL, MySpace, and Yahoo! participate with the National Center for Missing and Exploited Children in disseminating reports on missing children.
- **Educational Resources:** All eight of the social network sites who submitted to the Task Force offer educational resources and online safety tips for their users.

The submissions themselves, attached in Appendix E, provide much greater detail about these and other efforts being made by the social network sites, and should be read in tandem with this Report.

VI. Analysis

A. Background

The Task Force began with the premise that in order to determine how today's technologies can help promote online safety for minors, it is important first to have a clear understanding of the actual risks that minors face online. Taking the risks outlined by the Research Advisory Board in its presentations and in the Literature Review as the starting point, Task Force members considered information about the submitted technologies to determine the extent to which any category of those technologies could assist in addressing specific risks. The Task Force was limited to studying those technologies submitted through the process established by its Technology Advisory

Board, though individual members sought out other approaches in university labs and in development at corporations for background consideration. The Task Force recognizes that there is further, ongoing technological innovation taking place in both academic and corporate settings that was not brought to its attention, in part due to the public nature of the Task Force process and, in particular, the Task Force's Intellectual Property policy, which required public disclosure of all submissions.

No single technology submitted to the Task Force is purported to solve all of the disparate problems that minors face online or even to eliminate completely any one risk. Instead, each technology seeks to address specific aspects of safety for minors in particular online contexts, often with significant parental or caregiver involvement. Moreover, a technology or combination of technologies designed for one environment or for use by one type of service provider may not be able to provide the same level of effectiveness in a different context. Each site has its own unique architecture, equipment, and operations, so integration of new software requires careful planning and testing in order to avoid unintended consequences or even site outages. Thus, any technological approach must be appropriately tailored for the context in which it operates, given the wide range of services on the Internet. Finally, not all risks identified by the Research Advisory Board are addressed by a technology submitted to the Task Force for review.

At the same time, many potential technological solutions give rise to legal and public policy considerations, particularly if subject to government requirements. Though a full analysis of these legal and public policy concerns is outside the scope of this Task Force and is better left to key public sector and private sector stakeholders, the Task Force urges that they be taken into account prior to use of any particular technology. Some technologies may offer improved safety, but may have harmful public policy consequences and unintended consequences for youth and parents that outweigh the safety improvement. A balanced perspective is particularly critical in light of the Internet's central role in enabling freedom of expression and access to information from around the world.

Additional issues are raised by the global nature of the Internet. The Task Force's mandate was focused primarily on technological solutions to online safety for minors in the United States. The Internet, on the other hand, is international, with services, sites, and users that transcend national boundaries. This has important ramifications for understanding the potential benefit of any technological approach to online safety for minors. If a technological solution is put into place for a given social network site or service provider, a user may choose to use a different site or service, including one based outside of the United States and therefore subject to different laws and protections. This may be particularly true for minors, who tend to be at the forefront of finding new, uncharted online spaces to explore and seek out spaces that give them maximum freedom. Pushing minors – especially at-risk minors – into these alternative environments may well result in a net loss for youth online safety. At the same time, to the extent that social network sites and others adopt technological safety solutions that are incompatible with users from outside the United States, we risk closing our youth off from valuable interaction with the rest of the world. Finally, even if technological measures appear to

eradicate visible problems, they may not help at-risk minors who are engaged in risky online behaviors. Pushing those practices underground may complicate efforts to identify and serve the needs of at-risk youth. Given the Task Force’s focus on the United States, we did not study regulations or industry policies in place outside of the United States.

The Task Force remains optimistic about the potential for technologies to play a role in enhancing safety for minors online, but – consistent with the guidance of the TAB – cautions against over-reliance on technology in isolation or on a single technological approach. Instead, used in combination with education, parental involvement, law enforcement, and sound policies by service providers, a technology or combination of technologies may help to reduce some risks minors face online.

B. How the Technologies Address Risks Identified by the RAB

Below, the Task Force uses the three broad categories of risks facing minors presented by the Research Advisory Board and considers the relative promise of the submitted technologies in each instance.

1. Sexual Solicitation and Internet-Initiated Offline Encounters

Most of the technologies submitted to the Task Force for review are intended to reduce, to some extent, the risk of sexual predation on minors by adults. Some seem to presuppose that deception as to age is a core contributor to sexual solicitation, yet the research suggests that this is not a prominent or common issue in solicitations that lead to sexual encounters. The data outlined in the Literature Review show that in most incidents of Internet-initiated offline encounters between adults and minors, the minor knows that the adult is older (usually in his or her twenties), knows that sex is desired, and believes that she or he can consent to a sexual encounter. Many solutions also assume that sexual solicitations that youth receive always come from older adults, even though almost half of solicitations are known to come from other minors and most of the rest come from adults who are between the ages of 18–25.

a. Identity Authentication and Age Verification

The area of greatest focus of technology developers, and corresponding innovation, is in the related areas of identity authentication and age verification technologies. Most technological approaches that were submitted in this area focus on the authentication of adults only.

Relative to certain other forms of technologies submitted, these approaches have been developed over a longer period of time and some have been in widespread commercial use in many fields. For instance, identity authentication is used today to facilitate commerce via the Internet in financial and medical services, e-commerce, and the sale of age-restricted products and services. Under Section 326 of the USA PATRIOT Act, certain financial institutions are required to implement a Customer Identification Program that includes verifying a customer’s identity; the date of birth is listed as one of

the data points the financial institutions should gather. In addition, these technologies are used today to seek to ensure that those who purchase regulated items (such as alcohol or tobacco) or access adult-related content have a valid identity and are of a certain age.

However, these approaches are less effective in the child safety context – in other words, at creating safe environments for minors – than in the context of completing financial transactions or regulating purchases, especially to the extent that identity authentication and age verification focus solely upon adults. The reasons for this include the fact that in the commercial and financial contexts, an adult typically wants to verify his or her identity correctly in order to purchase a product or get access to records. **[The Task Force Report admits that AVS/IDV are widely used and work when people want to be known for who they are. And it is MySpace's position that it is popular because people want to be known just as in the real world. [See Nigam video, 9/24/08]**

But the Report contradicts both itself and MySpace, with inconsistent policy (not technical) arguments as to why SNS would not be good places for AVS/IDV. The Report seems to be saying that SNS such as MySpace should be geared toward those who don't want to be known, like convicted sex offenders, when the SNS themselves are saying that they are geared toward those who want to be known – that is, the very group for whom the Report acknowledges AVS/IDV would be most effective. See also the discussion above about IDV working in tandem with RSO removal technology to make such removal far more effective.] Moreover, when adults purchase regulated items (such as alcohol or tobacco) online, in some cases a second form of age verification occurs when the item is delivered.

The identity authentication and age verification solutions that authenticate or verify only adults could be and are already sometimes used to reduce minors' access to adult-only sites. Because they do not authenticate or verify minors, however, they cannot be used to create environments for minors that require authentication or verification prior to access. To the extent that an adult nonetheless uses his or her own verifiable information when accessing an environment intended only for minors, these technologies could enhance the ability of Internet service providers and social network sites to exclude that adult. Of course, it seems unlikely that an adult with nefarious purposes would proceed in this manner. Thus, while these types of identity authentication and age verification technologies may be helpful for other purposes, they do not appear to offer substantial help in protecting minors from sexual solicitation.

Some of the technologies submitted would establish a system for authenticating the identity and/or age of minors as well as adults. Those technologies are intended to allow for the creation of environments intended only for minors for which authentication is required prior to access. Thus, adults – or some adults, such as registered sex offenders – could be excluded. Such a technology is more likely to allow for dedicated spaces online in which minors would theoretically have greater protection from sexual solicitation by adults than they would have elsewhere on the Internet, although concerns

with that concept are noted below. The technologies that seek to authenticate minors' identities rely on verification by various means, including biometric devices, peer rating systems, and school-based authentication, each of which carries its own expense and challenges, as noted below.

Some Task Force members expressed a range of concerns – some of which also were noted by the RAB or TAB – with identity authentication and age verification technologies for both adults and minors. These concerns include:

- The authentication and verification technologies that validate login IDs or credentials for adult and/or minors could be subject to circumvention by users who trade or distribute IDs or credentials. Unlike in financial contexts, users in online social settings may have reduced incentives to maintain the confidentiality of login IDs and credentials, and members of the RAB report that sharing credentials is common among young people. Moreover, there is a risk that the use of IDs or credentials could lead to a “black market” for them, in which (hypothetically) an adult could acquire a credential allowing them into an online area intended for minors.
- Technologies that seek to authenticate minors' identities relying on verification by biometric devices, peer rating systems, and school-based authentication all involve financial costs, especially if they must be implemented broadly to have an effect.
- Relying on schools to assist with the verification of minors would place a new burden on an educational system that is already unable to meet its goals based on current levels of funding, staffing, and support. In addition, federal and state laws restrict the ability of schools to provide certain personal information about minors to third parties, without requisite consent, which complicates school verification processes.
- Reliance on peer ratings for verifying minors, as the TAB noted in its report, could increase forms of bullying.
- Relying on parents and caregivers for verification presumes that all minors have healthy relationships with their parents and that parents are not themselves engaged in illicit activities. As discussed in the Literature Review, this is not always the case. Many children have unhealthy family dynamics and adults involved in crimes against children frequently have offline connections with minors. There is a risk that adults with nefarious purposes could register a minor in their charge and use that account to get access to a purportedly safe space where minors and their parents have relaxed their guard.
- The scope and effectiveness of some authentication and verification technologies may be limited in the context of the global Internet, with sites that welcome and encourage visitors from across the world to interact with one another. Many of the

technologies are based on public records or social structures that are primarily found in the United States, and thus the technologies may not be able to verify or identify non-U.S. visitors to websites, including social network sites. This could lead to users leaving U.S. sites for less restrictive sites, or to users in the United States being isolated from the global discussion of issues of concern.

- The exclusion of all adults from a site by means of identity authentication and/or age verification technology would not eliminate many of the risks of sexual solicitation. None of these technologies account for the fact that minors usually choose to connect with adults, and indeed, many of the most popular online social sites are by design places where older minors and adults can communicate. In addition, sites that seek to exclude adults would not prevent the risk identified by the RAB that minors sexually solicit other minors.
- Not all interactions between adults and minors are unhealthy and potential solicitations. Many technologies do not account for the frequency with which minors interact with adult family members, teachers, and mentors online, or the frequency with which teenagers have friends who are over 18. Minors gain benefits by being able to engage in healthy and supportive interactions with adults, including known adults and adults who are participating alongside youth in communities of interest. In addition, excluding parents from a site could reduce their ability to monitor their children's use of the site, which could increase other problems, such as online harassment and bullying. Excluding teachers and other role models from sites could have unintended consequences for learning and development.
- To the extent that these technologies do allow "trusted adults" access to a site that otherwise was dedicated to minors, it is unclear how a determination that an adult falls into that "trusted" category is to be made. Given the RAB's data that most sex crimes are committed by family members or offline acquaintances, including neighbors, friends' parents, leaders of youth organizations, and teachers, it seems unwise to allow all parents and caregivers access to sites intended only for minors. Moreover, lack of a criminal record or sex offender status is in no way an indication that the individual is in fact worthy of trust; many perpetrators simply have not been caught.
- There is a concern that some technology companies will sell information that they collect on minors to advertisers or otherwise target advertising to specific children or age groups. This concern is not limited to age verification and identity authentication technologies.
- The authentication and verification technologies submitted present privacy and security concerns, at least in theory.

b. Text Analysis, Individual Profiling, and Filtering and Monitoring Technologies

Other technologies that address the risk of sexual solicitation online include text analysis, individual profiling, and filtering and monitoring technologies.

Text analysis technologies are designed to detect predatory, bullying, or otherwise inappropriate conversations on the Internet. Text analysis has the potential to address many more of the risks involved in sexual solicitation, including solicitations between minors and those in which minors are active participants. The TAB has indicated that although these technologies are promising, the submissions received were at an early stage of development. No technology in this category appeared ready for widespread use. It is possible that parents could use some form of text analysis to assist in monitoring their child's interactions with others, but even that process contains a host of privacy- and security-related concerns that should be taken into account, especially when children are in unsafe households.

Individual profiling is a category of technology that endeavors to prevent certain categories of individuals, such as registered sex offenders, from gaining access to a given website or areas of a given website. This approach is an example of "selected exclusion," or disallowing access to those who meet certain criteria, rather than "selected admission," or admitting users based upon certain criteria (as in the case of identity authentication and age verification technologies). A selected exclusion approach, such as the removal of suspected registered sex offenders, can help to reduce unwanted contact between minors and sex offenders by limiting access to sites by the individuals who are profiled. This approach involves using identification mechanisms beyond the basic pedigree information that offenders will enter when registering for a site. As discussed previously, MySpace is presently working with one of the technologies submitted in this category.

As with other technologies, some Task Force members expressed concerns about limits to the effectiveness of such an approach:

- First, the database with information on a given individual must be accurate and the individual must seek to access the site using that information. It seems likely that at least some registered sex offenders and other individuals who are profiled would seek to circumvent this system if they had nefarious intentions.
- To the extent that a profiling technology focuses on registered sex offenders, it cannot prevent access to sites by individuals who prey on minors but have not yet been caught, convicted, and registered. In this way, the limitations of these technological approaches mirror the real world, as law enforcement officials cannot stop crimes that they do not know are being committed.
- This type of technology may not keep out those who have been removed from the site but sign up again using a different identity. Conversely, this approach may limit the access of those who have legitimate reasons to be on social network sites. Technology providers contend that they have developed effective means to reduce the incidence of both of these problems.

Despite these concerns, the Task Force heard praise for the continued promise of technology in finding and removing registered sex offenders from Internet sites.

The Joint Statement references a plan by MySpace to explore the establishment of email registries for children. The TAB received a few submissions with email registries for children as a component, one of which was withdrawn by the submitting company, and considered these in its assessment of age verification and identity authentication technologies. The Task Force did not focus extensively on this concept, but notes that there are a host of civil liberty, privacy, and safety concerns with collecting information on children for a registry of this sort.

To the extent that they prevent minors from accessing certain sites that are deemed less safe than others by parents or third parties, filtering and monitoring technologies, sometimes referred to as “parental control” technologies, also may help reduce the risk of sexual solicitation involving younger children in particular. These technologies are discussed in greater detail below.

2. Online Harassment and Cyberbullying

Although the RAB has identified online harassment and cyberbullying as the most common risk that minors face, few technological solutions have been proposed to address these issues directly. Because so much of this activity takes place between minors who know one another, it is unclear that any of the technologies submitted to the Task Force presented would have a substantial impact in terms of reducing how often it occurs or its severity. The problem is further complicated by frequency of reciprocal harassment, blurring lines between victims and perpetrators, and the ways in which bullying moves between online and offline contexts and between different forms of social media.

Some Task Force members suggested that large-scale adoption of identity authentication for minors and adults alike, across all Internet services, could lead to more accountable behavior online, which in turn might result in less online harassment of minors. Even such a large-scale approach would not be foolproof, however. After all, young people who know each other bully one another face-to-face and, more often than not, victims of online bullying know who their harassers are.

Text analysis technologies also could address this problem by allowing for greater monitoring of communications between minors. As discussed earlier in this report and in greater detail in the TAB Report, these technologies carry many technological hurdles, as well as legal and privacy concerns. Additionally, many types of bullying cannot be detected through text, including those involving impersonation, password stealing, and the distribution of embarrassing images and video. Also, often the distinction between content that is part of social discourse and that which is harmful is context-dependent and technology is unlikely to be able to effectively recognize the “rumors” and “gossip” that make up the bulk of online harassment. At younger age-levels, monitoring features of parental control software could help provide parental insight and involvement into

bullying situations. Text analysis may also be able to help psychologists and social workers address the problem.

3. Exposure to Problematic Content

As outlined by the RAB, problematic content raises two separate technical issues: (1) unwanted exposure by minors who are unwittingly exposed during otherwise innocuous activities; and (2) minors' ability to access content that they desire but that their parents do not want them to be able to access.

Filtering and monitoring technologies are perhaps the most mature of all of the technologies considered by the Task Force. These tools include the parental controls that are available through most Internet service providers. These tools can be and have been implemented by schools, libraries, and parents to limit minors' access to some categories of problematic content. Filtering and monitoring technologies are a useful tool to assist parents and other responsible adults in determining their children's access to appropriate Internet content, particularly for younger children. They are, however, 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. Minors can circumvent these technologies most simply by using the Internet at friends' houses or in other places that do not use such technologies. Also, many handheld devices, such as gaming devices, have WiFi capabilities, and unsecured wireless networks can be accessed in the child's bedroom, backyard, or elsewhere, allowing for greater opportunity to bypass parental controls. Increasingly, minors are also learning how to use proxies to circumvent filters or to reformat their computers to remove parental controls. 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.

Filtering technologies are also limited in their scope. To date, most filtering technologies focus on sexual context and inappropriate language. Some fail to restrict access to violent content, hate content, and self-harm content. They also fail to address the rise of youth-generated problematic content distributed virally. Most filtering technologies do not yet address video- and image-centric content or content distributed over mobile phones.

Identity authentication tools that allow for the creation of adult-only environments from which minors are excluded can help to curb minors from accessing certain types of problematic content. That presupposes, however, that minors are not using verification information from their parents or other adults (or their own credit cards) to get into such an adult-only environment. Some identity authentication tools deploy interactive dynamic knowledge based authentication that makes misuse of parental information more difficult, but savvy teens can often answer these questions. Of course, these adult-only spaces are just one small part of the Internet as a whole, tend to cover only commercial adult content, and would not protect minors in any other context.

C. A Note on Technologies Not Submitted to the Task Force

The Task Force takes note of omissions from those technologies that it was presented with for review. A few areas deserve special mention.

First, there are many broad-based identity authentication technologies in development at universities, small companies, and large companies that might complement those specific technologies presented to the Task Force. Some of these authentication efforts are open source or based on open standards; others are proprietary. Examples of such identity technology efforts include OpenID, the Higgins project, and others described at <http://informationcard.net> and <http://www.eclipse.org/higgins/>.

Second, few submissions to the Task Force focused on technology tools that law enforcement officials – whether investigators, prosecutors, or computer forensics specialists – might use in their work. Of course, many such technologies are in use today. The Task Force notes that innovation in this area could provide enormous benefits to online safety for minors, both in terms of deterrence and in bringing wrongdoers to justice and keeping them out of online and offline spaces where minors congregate.

Third, the TAB did not receive any submissions from technologies specifically intended to prevent access to child pornography. Because it is illegal throughout the United States even to possess images of children being sexually abused, the appropriate focus with child pornography is on preventing not just minors, but also adults, from accessing it. Use of the filtering and monitoring technologies discussed earlier could help protect some minors from access to child pornography, with the limitations already noted. As indicated in Part V above and in the submissions in Appendix E, some of the social network sites themselves are working on this problem. Under recent federal legislation, the National Center for Missing and Exploited Children may provide “elements relating to any apparent child pornography image of an identified child,” including “hash values and other unique identifiers,” to service providers, which may encourage greater development in this area. (18 U.S.C. § 2258C(a) (2008)).

Fourth, the TAB also did not receive any submissions from technologies specifically intended to prevent youth from creating and distributing sexual content of themselves or their peers. Finally, no submissions focused on tools that could help social services work to identify and protect at-risk minors.

Any subsequent review should take into account more of these efforts, which have not been explored in detail by this Task Force.

VII. Recommendations

The Task Force does not believe that the Attorneys General should endorse any one technology or set of technologies to protect minors online. While the Task Force understands the desire to find a solution and recognizes that technology plays a significant role in enhancing online safety, our review found too little evidence that any given technology or set of technologies, on their own, will improve safety for minors

online to any significant degree. Moreover, the Internet itself, the ways in which minors use it, and the communities in which they participate all change constantly, and the available technologies are quickly evolving. The Task Force believes that the Attorneys General have played a key role in bringing national attention to the issue of online safety for minors, driving significant innovation and creativity in the area of child online safety. The Task Force is concerned that endorsement of any one technological approach would stifle future progress in this area.

The Task Force believes that the Attorneys General should continue to work collaboratively with all stakeholders to help enhance safety for minors online and reach out to some – like those involved in mental health and social services – who are not currently involved in helping find solutions to protect minors online. The Attorneys General are in a unique and important position to help guide efforts to help keep online communities safe for minors. Of course, any use of technology to enhance safety for minors online must be in tandem with education, industry adoption of best practices, and the involvement of social services and law enforcement, in all of which the Attorneys General can play a crucial role. At the same time, the Task Force makes the following recommendations for the Internet community, recommendations regarding allocation of resources, and recommendations to parents.

A. Recommendations for the Internet Community

1. Members of the Internet community, including social network sites, should continue to develop and incorporate a range of technologies as part of their strategy to protect minors from harm online. They should consult closely with child safety experts, mental health experts, technologists, public policy advocates, law enforcement, and one another as they do so. But they should not overly rely upon any single technology or group of technologies as the primary solution to protecting minors online. Just as there is no single solution to protecting minors online, any technological approach must be appropriately tailored for the context in which it operates, given the wide range of services on the Internet. Parents, teachers, mentors, social services, law enforcement, and minors themselves all have crucial roles to play in ensuring online safety for all minors – and no one's responsibility to help solve the problem should be undervalued or abdicated.
2. Members of the Internet community, including social network sites, should continue to work together as well as with child safety experts, technologists, public policy advocates, social services, and law enforcement on the development and combination of the most innovative and promising technologies; setting standards for the use of technologies and the sharing of data, as needed; and identifying and promoting best practices on how to implement technologies as they emerge and as problems facing minors online evolve. In so doing, they should take into account what types of tools would be most effective for law enforcement and social services to use in enhancing the safety of minors online.

3. Prior to implementing any type of technology designed to address safety for minors online on a broad scale, the Internet community should carefully consider what the data show regarding the actual risks to minors' safety online and how best to address them, paying close attention to the most at-risk youth.
4. Prior to implementing any type of technology designed to address safety for minors online on a broad scale, the Internet community should carefully consider users' constitutional or other rights, including freedom of expression and access to information, as well as privacy and security concerns.
5. Prior to implementing any type of technology designed to address safety for minors online on a broad scale, structures should be put into place to measure the effectiveness of the technology at solving the existing problems and all such data and analysis should be consulted. No technology should be implemented without a deep understanding of its effectiveness at addressing the risks minors face and understanding any unintended consequences presented by that technology.
6. As technologies designed to address safety for minors online develop, particular attention should be paid to ensuring the safety of at-risk youth, including those for whom positive parental involvement is not a given, those for whom cost is an issue, and those who are engaged in risky behaviors and may themselves contribute to the problem. Making sure that agencies, institutions and experts addressing at-risk youth are included in the discussion and evaluation of technological approaches is essential. For the same reasons, attention should be paid to ensuring that technologies are accessible to parents and caregivers with little or no experience in using technology and with limited understanding of the risks being addressed, and that non-English-speaking and functionally illiterate parents are given tools and guidance to address safety issues.
7. All technologies designed to address online safety for minors should take into consideration the international nature of the Internet. Any consideration of the Internet from an international perspective should take into account how other countries address online child safety and how cooperation can facilitate a safer international community.

B. Recommendations Regarding the Expenditure of Resources

1. To complement the use of technology, greater resources should be allocated to schools, libraries, and other community organizations to assist them in adopting their own risk management policies and for educating children, parents, and caregivers on issues relating to online safety.
2. To complement the use of technology, greater resources should be allocated to law enforcement for training and developing of technology tools to enhance law enforcement officers' computer forensic skills; to develop online undercover

operations; and to enhance community policing efforts to educate minors, parents, and communities about youth online safety.

3. To complement the use of technology, greater resources should be allocated to help social services and mental health professionals who focus on minors and their families, including social workers and guidance counselors, to extend their practice and expertise to online spaces. Resources should also be provided to help these groups 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.
4. To complement the use of technology, greater resources should be allocated for ongoing research into the precise nature of the risks facing minors online and how this shifts over time and is improved by interventions. As set forth in greater detail in the Literature Review appended to this report, there is a need in particular for longitudinal studies that track minors across multiple domains. There is also a need for researchers and the public to gain a better understanding of the data that law enforcement officials are gathering through their work in the field. In order to allow for more systematic and thorough research, law enforcement should work with researchers and provide access, where possible, to data on offenders. One way to accomplish this goal would be to collaborate with the American Correctional Association to include questions about online activities in interviews of convicted sex offenders. In addition, data on the online practices of registered sex offenders should be maintained by technology companies and appropriately anonymized data should be made available for study where legally and technically possible.

C. Recommendations for Parents and Caregivers

1. 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. A list of resources is available at <http://cyber.law.harvard.edu/research/isttf>.
2. Parents and caregivers should explore and evaluate the effectiveness of available technological tools for their particular children and family context, and adopt those tools appropriately. The technologies submitted to this Task Force – especially the well-developed field of parental controls technologies – form the starting point for this exploration, guided by the evaluation begun by the Technology Advisory Board and the Task Force as a whole.
3. Parents and caregivers should be engaged and involved in the Internet use of their children, discussing it from an early age, setting appropriate limits and instilling good behavior from the start. Being attentive to early signs of harassment, both in terms of children as bullies and victims, is critical, especially because bullying tends to escalate over time.

4. Parents and caregivers should be conscious of the common risks that minors face and avoid focusing on rare or hypothetical dangers. Their strategies should center on helping their children understand and navigate the technologies and creating a safe context in which their children will turn to them when there are problems. Trust and open lines of communication are often the best tools for combating risks.
5. Parents and caregivers should be attentive to at-risk minors in their community and in their children's peer group, especially because youth frequently make their risky behaviors visible to their peers. Helping other at-risk minors get help and support benefits all online youth.
6. Parents and caregivers should recognize when they need to seek help from schools, mental health professionals, social services, law enforcement, and others regarding use of the Internet by their children. **[As noted above, to give families the tools they need, notice should be given to the user, and to the parent if known, the instant that an SNS has information that a child has even been contacted by an RSO. Such contacts should never, ever be presumed innocent. We have community notification in the real world whenever an RSO moves into the neighborhood. If there is good reason to sit on this information, such reason should have been included in the Report. The Final Report's complete silence on this issue – an issue raised repeatedly by Aristotle during the public and private Task Force meetings -- is incomprehensible to us.**

If there are laws that prevent an SNS from providing the Task Force with any information on the use of their site by RSOs (even in the aggregate), or from taking obvious steps to protect children (such as giving notice when an SNS learns that a RSO has contacted a minor child), this should have been addressed by the Task Force so that various options could be considered.]

VIII. Conclusion

The Internet Safety Technical Task Force is grateful to have had this opportunity to advance the understanding of the risks to online safety for minors and to assess how today's technologies can play a role in enhancing it. The Task Force thanks the Attorneys General for their leadership and the many volunteers who contributed their time, energy, and insight to this compressed review process. The Task Force concludes our work optimistic that collaboration and innovation in this field will continue in ways that will directly benefit of the safety of children.

ⁱ [Self-Evident Limitations in the Exploratory Research Presented to the Task Force](#)

Several specific limitations in the research should be noted, if only because they are self-evident. By way of example, we focus on the Ybarra/Mitchell study in *Pediatrics* (Ybarra and Mitchell 2008) that was presented at the first public meeting of the Task Force, and cited several times in the report. The study is based on an online survey of 1588 minors aged 10-15 years old. We have identified above only what we consider to be the most obvious concerns affecting the “probative” nature of such research.

a) The Exploratory, Non-Probative Nature of the Study

It appears that the authors used only frequency analysis in their study. This is an elementary statistical technique that is exploratory in nature. To answer a more direct question of whether harassment/victimization is more common in social networking sites than other online sites, the authors would need to do regression or other more sophisticated techniques, adjusting for potentially confounding factors.

b) Skewed Age Range of Those Surveyed (10-15 Year-Olds)

In “Online ‘Predators’ and Their Victims” (Wolak 2008), the researchers make several important claims:

- i. *[A]s youths get older and gain experience online, they engage in more complex and interactive Internet use. This actually puts them at greater risk than younger, less experienced youths, who use the Internet in simpler, less interactive ways. Among youths 12-17 years old, it was those 15 to 17 years of age who were most prone to take risks involving privacy and contact with unknown people.* (p. 115)
- ii. *“99% of victims of Internet-initiated sex crimes in the N-JOV {National Juvenile Online Victimization 2003} study were 13-17 years old, and none were younger than 12”.* (p. 115)
- iii. *Boys constitute 25% of victims of Internet-initiated sex crimes* (meaning that 3 times as many girls are victims than boys) (p. 118)

From the face of this research, therefore, it makes little or no sense for us to report anything from the Ybarra/Mitchell survey of 10-15 year olds as even arguably probative about the number of unwanted solicitations of all minors on SNS. That survey excludes most of the highest “risk-taking” group (16-17 year-olds), and skews the results on frequency of such contacts even further downward by including the least “risk-taking” group (10-12 year olds). For all we know, the figure of “4% of all youths reporting an unwanted sexual solicitation on a social networking site” could actually be 25% or 30% for 15-17 year olds on SNS. Among girls alone (the more victimized gender), the figure would be even higher. Given how many teen users there are, this percentage could represent an extremely large number of affected teens.

It was important that the report to the AGs not selectively use quotes or figures from the research to minimize the problem of predation on SNS. The studies and articles presented contain ample evidence of potentially troubling conditions. Again, even as the authors of Wolak 2008 themselves note, with reference to Ybarra and Mitchell 2008, “*caution should be used in interpreting this small amount of research about a new phenomenon*” [the risk of sexual victimization through use of SNS such as MySpace]. As noted above, this disclaimer -- which is central to the issue the Task Force was supposedly examining -- never found its way into the Final Report, despite repeated requests by Aristotle for its inclusion to show some sense of balance.

c) Lack of Confidentiality

The adults apparently completed a brief survey and then “handed the survey to youth” for completion. There was no promise of confidentiality to the children. The parents may have been in the room with the children while they completed the survey, may have helped their children complete the survey, or may have insisted on reviewing the survey. All of these possible scenarios could have affected how truthful the children were in their responses. If anything, this would likely have decreased the amount of victimization and/or harassment that the children reported.

An incident reported in *The Atlantic* underscores this point:

As part of the first episode of his show [To Catch a Predator], [Chris] Hansen convened a panel of tweens and teens, among them children of some of his colleagues at NBC, and asked how many of them had been “approached online by someone in a sexual way that made you feel uncomfortable.” Almost all the kids raised their hands. Then he asked how many had told their parents. Not a hand went up. And when he asked why they hadn’t told their parents, all the kids in the room said they didn’t tell because they didn’t want their parents to take away their Internet connections.

See “Babes in the Woods”, <http://www.theatlantic.com/doc/200707/myspace> (emphasis added). Without confidentiality of responses, there is no reason to believe that children in the Harris Poll survey reacted any differently than the group described here.

d) Only “Unwanted” Contacts Are Recorded

This paper does not address what is clearly a broader problem inherent in social networking sites: the sexual solicitation of a minor by an adult when the minor plays a willing or participatory role. The survey never asks about whether the minor formed a relationship with an adult and was later assaulted/victimised/harassed. Furthermore, the ‘level’ of victimization or harassment is unknown. A child on a social networking site might encounter more ‘serious’, ‘aggressive’ or ‘threatening’ harassment than what might be encountered through e-mail, for example. Victimization or harassment by a stranger, also, is likely to differ from harassment by someone you know not only in the fear it provokes but in how the child reacts to the threat.

e) Controlling for Consistency in Questioning

It is well-known that when conducting a population-based survey such as this with non-clinical interviewers, it is very important that participants are all asked the same questions, in the same manner. Survey methodologists spend a great deal of time on the precise wording of each question. When a respondent does not understand a question, the non-clinical interviewer cannot interpret the question for the respondent. In this case, by putting the parents’ own “spin” on the question, a “standardized” instrument becomes non-standardized. In this particular survey, it is very likely that children may have been confused as to the meaning of the questions, which would be expected when asking a 10- or 12- or 14- year old about sexual “solicitation” and “harassment” and other words and concepts they may not be very familiar with yet. They then may have asked their parents for clarification. If these parents were doing this, then it is likely to change the meaning of the question for each child, and therefore make the responses to the questions unable to be compared across children.

f) The Population Surveyed

The population of parents was obtained through a Harris Poll Online opt-in panel with a response rate that appears very small (26%). The authors state that this is acceptable for online surveys.

However, our understanding is that it is likely that epidemiological studies seeking to determine true associations of health- and behavior-related events in the populations would not find this to be an acceptable sample.

It also is likely that this sample of Harris Online Poll parents still differs dramatically on many *unmeasured* factors that are particularly relevant for the examination of children's internet usage and victimization/harassment, including parenting style, parental personality, parental work schedule, number of other children in the house, parental knowledge of the internet, location of child's computer (e.g., family room vs. child's bedroom), number of parents in the household, presence of psychiatric disorders in parents or children, child IQ, school performance of children, children's participation in extracurricular activities, etc.

g) Time Period Covered by Survey

Youth were asked about unwanted sexual solicitation and harassment occurring within the last year [See Study Table 4]. This paper addresses what is considered "current" harassment. It is possible that many more youths would have reported harassment/victimization if the question was worded to examine "any" harassment/victimization in their past. In epidemiological studies, "lifetime" rates are always higher than 12-month rates. This study concludes that "4% of youth reported an unwanted sexual solicitation on a social networking site", but this is only within the past year and says nothing about previous encounters.

h) Troubling Statistics Omitted from Final Report About Unwanted Sexual Solicitations Of More Frequent SNS Users,

Even with all of the questions about the research methodology and the "hypotheses" offered, the exploratory studies presented to the Task Force actually contain some troubling statistics and comments about more frequent users of SNS.

Example:

Table 3 of the Ybarra/ Mitchell 2008 study in *Pediatrics* shows that 248 of the surveyed 10-15 year olds said that use of SNS was one of two activities they spent most time doing when online. Of these 248, there were 72 (or 29%) who reported unwanted sexual solicitation. This troubling statistic was presented to the Task Force in the research, and is far greater than the frequently mentioned 4% figure. These numbers should have been included for balance in the Final Report.

ⁱⁱ *AG creates cybercrimes unit to battle illegal online activities,*
<http://www.wave3.com/Global/story.asp?s=8437905>