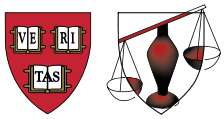
Enhancing Child Safety & Online Technologies:

FINAL REPORT OF THE

INTERNET SAFETY TECHNICAL TASK FORCE

To the Multi-State Working Group on Social Networking

of State Attorneys General of the United States



Berkman

The Berkman Center for Internet & Society

at Harvard University

DECEMBER 31, 2008

Appendix F:

Statements from Members of the Task Force

AOL and Bebo's Statement Regarding the Internet Safety Technical Task Force's Final Report

AOL and Bebo would like to thank the Berkman Center and all of the Task Force members for their work in developing a well thought-out report that accurately identifies the major online threats to children, analyzes the causes of those threats and fairly evaluates specific technologies designed to mitigate certain dangers. Though we do not agree with every aspect of the report, we do agree with its general findings.

Long before the recent attention to safety in the context of social networking services, the online industry actively promoted technologies and tools to protect children. More than a decade ago, AOL first introduced parental controls, and since that time has demonstrated its long-term commitment to child safety by deploying a broad set of solutions that combine technology, monitoring and reporting, education, and cooperation with law enforcement. AOL remains strongly committed to making the Internet a safer place for our families.

Today on Bebo, AOL's social networking site, in addition to deploying a range of safety solutions, we are also striving to address the vulnerabilities that may contribute toward a young person being exploited online As the Task Force report demonstrates, teenagers going through difficult phases in their lives are far more vulnerable to danger, both off- and online. To address these vulnerabilities, Bebo has developed Be Well (www.bebo.com/bewell), a platform for mental health support groups to engage with its users. Bebo believes that social networking sites are uniquely positioned to help address many of the dangers currently facing young people, by helping teenagers gain access to support services from within an online community, thereby de-stigmatizing help seeking and facilitating early intervention. Putting the support services that minors need to navigate life's challenges at their fingertips can result in well-informed, better-prepared teens who are less vulnerable to predators, bullies and other off- and online dangers. Many challenges still remain to using these new technologies to their fullest potential, including ensuring that essential ethical and professional practice principles concerning client welfare, confidentiality, competence, responsibility, and integrity are upheld. To address these and other issues, Bebo is chairing a multi-stakeholder group to develop Best Practice standards (information available at www.technologyforwellbeing.ie).

In conclusion, we would like to reiterate a vital concern expressed by the Task Force. The "*endorsement of any one technological approach would stifle the innovation and creativity that has begun to flourish…"* (p. 33). We are just beginning to harness the potential of the Internet to transform the accessibility of support services, and to help reduce the vulnerability of many teens, particularly those who do not have family support. It would be counterproductive to that progress to enforce any specific technology mandates or blanket prohibitions. Such policies would serve only to exclude many at-risk teens from vital support services, and leave many other children less prepared to face risks that occur both in the real world and on the Internet. Instead we urge policy makers to encourage the continued innovation and evolution of safety strategies – both reactive and proactive – that providers are developing.

Aristotle International: 12/19/08 Statement on ISTTF Final Report to Attorneys General

- The Final Report of the MySpace-funded Task Force ignores MySpace's ongoing destruction of data about how 50,000+ Convicted Sex Offenders (CSOs) have been using the giant SNS, which claims 8.5M users under age 18 in the U.S.
- Report fails to mention that the data on 50,000+ CSOs found on MySpace in the last year was not even requested for study. This omission casts the Task Force's focus into serious doubt. *Concerned parents, Attorneys General, and others will wonder how a Task Force with a research group, all supposedly devoted to focusing on SNS safety, could fail to ask for such highly relevant data.*
- MySpace told the Task Force that it has no idea how many of its 100M+ users have registered with their real identities. The Report does not mention this fact.
- The AGs asked the Task Force to "focus on finding and developing online identity authentication tools," primarily for SNS in the US. *Objective not met. The Report barely mentions technical evaluation of authentication tools for SNS.*
- The AGs asked the Task Force to "establish specific and objective criteria that will be utilized to evaluate existing and new technology safety solutions." *Objective not met. Instead of establishing criteria as requested, the Report concludes that "developing standard metrics for youth online safety solutions would be useful".*
- The Report grossly overstates what the research tells us about SNS. Most is pre-SNS or preliminary, very early qualitative research on hypotheses that have not been thoroughly tested. It includes "online surveys" of 10-to-15 year-olds about sexual solicitation. There is little actual SNS research and none for CSOs on SNS.
- On the question of whether SNS such as MySpace increase the risk of victimization by online molesters, leading researchers warned in 2008 that "***caution should be used in interpreting this small amount of research about a new phenomenon***". The Report omits this warning and asserts that SNS do not increase risks.
- 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. *We must answer the technical questions we were asked as a* ***technical*** *task force, instead of acting primarily as self-appointed* ***policy*** *advisers. Study of CSOs on SNS must also begin without further delay, excuse, or filibuster.*
- Report fails to include proposed Aristotle recommendation concerning notice to teen (or parents) when SNS knows a CSO has contacted the minor on the site. (Proposal analogous to "community notification" for CSOs in the outside world).
- Three questions must be asked of MySpace: 1) Will it immediately offer researchers the data on the 50,000+ known CSOs' use of MySpace?; 2) Will it immediately stop destroying records of known CSOs' use of MySpace?; and 3) Will it notify minors/parents (changing TOS if needed) when it learns that they have been contacted by a CSO? (If not, we urge hearings/ AG investigations).
- A detailed, point-by-point analysis of the Task Force Report, plus links to many reports of sexual assaults on minors engineered through SNS, are available at **www.Aristotle.com/integrity/MySpaceTaskForce/sex-offenders-and-social-networks.** We also concur with the reasoned comments of IDology.

December 17, 2008

AT&T: Statement Regarding the Internet Safety Technical Task Force's Final Report to the Attorneys General

AT&T thanks the Berkman Center for its leadership of the Internet Safety Technical Task Force over the past several months. As the leading broadband communications provider in the US, AT&T joined this Task Force because we are committed to ensuring that families and children are safe and secure online and to safeguarding free expression on the Internet. While AT&T, and others on the Task Force, may not agree with every individual statement, finding or conclusion contained in the report, we strongly support the academic rigor and thoughtful analysis that the Berkman Center put into this report.

This report should be viewed as a significant milestone in online safety, not the final destination. On one hand, this report clearly shows that a significant amount of information is known about online safety issues. There has been and continues to be a wealth of academic research addressing the Internet's impact on youth – detailing the countless positive aspects along with the more troubling ones. Until now, much of this research has not been exposed beyond academic circles. One of the more important contributions of this report, therefore, is identifying and cataloging this impressive body of research and making it more widely available to law enforcement, policymakers and the general public. In addition, one of the key findings of the report is that kids do not differentiate between their offline lives and their online lives. As the report details, many of the same risks and challenges that youth face in the online world are an extension of the risks and challenges that they face offline. That is not to ignore the fact that there are some unique online challenges, but many of the techniques that we have used to address problems in the offline world have applicability online. While the Internet is a new frontier, it is not completely foreign territory.

At the same time, it's equally clear that ongoing research is needed to better understand online safety issues and develop effective solutions for protecting children. The Internet continues to evolve, posing new challenges and opportunities for families and children. Therefore, it is important to respond dynamically, not with static perspectives. While the existing research is impressive, it also points to the need for more research and more integration of multi-stakeholder solutions. Technology has played an important role in keeping kids safe and will continue to play a role in ensuring Internet safety, but, ultimately, effective online safety is a combination of awareness, education, technology, public health, law enforcement, and involved parenting. These elements must work in concert and be guided by facts and analysis.

Importantly, the work of the Task Force should provide an important foundation for a new set of government-led education and awareness efforts coming out of federal legislation enacted this past fall. AT&T looks forward to participating in these efforts and continuing to ensure that our customers are able to participate in a positive Internet community that is also safe and secure.

December 21, 2008

CENTER FOR DEMOCRACY & TECHNOLOGY
Working for Civil Liberties on the Internet

1634 I Street, NW Suite 1100
Washington, DC 20006
202.637.9800
fax 202.637.0968
http://www.cdt.org

Statement of the Center for Democracy & Technology Regarding the Internet Safety Technical Task Force's Final Report to the Attorneys General

The Center for Democracy & Technology (CDT) appreciates the opportunity to have served on the ISTTF over the past year. The Final Report appropriately concludes that the risks to children online are both more limited and of a different nature than the popular media has suggested, and that there is no one or group of technologies that will solve safety concerns. A critical conclusion of the Report is that legislatures and government officials should not *mandate* that social networks (SNs) implement online safety technology. The Report did not, however, spend much focus on the legal and policy concerns that would be raised by such a mandate.

Constitutional Concerns: A key threshold fact is that virtually all speech on social networks – even speech among minors or between minors and adults – is *completely lawful and constitutionally protected*, and predatory speech constitutes only a tiny percentage of the mass of vibrant, constructive speech that happens every day on SNs. Thus, any law or government mandate that would restrict or burden access to SNs would bear a strong presumption of unconstitutionality. Most of the technologies considered by the Task Force would, if mandated, erect unconstitutional obstacles to the ability of both minors and adults to access social networks or communicate online, and would also burden the constitutional right of online speakers to reach the broadest possible audience. Even minors have a constitutional right to be free from government interference with the ability to speak and listen to speech online.

First Amendment Framework: Under the framework set out in 1997 by the U.S. Supreme Court in the seminal *Reno v. ACLU* decision, online speech receives the highest level of First Amendment protection. Based on that decision, numerous courts over the years have struck down a broad range of laws that sought to protect minors online, because there are better and less burdensome ways to protect children. As this Task Force saw, there are a broad range of "user empowerment" tools that parents and caregivers can use to protect their children, and such tools (coupled with vital education of both minors and adults) represent a more appropriate and constitutional way to protect children in the online environment.

Privacy Concerns: Beyond the constitutional concerns that would be raised by a mandate to use a given technology, many of the technologies raise very serious privacy concerns, in particular by forcing the collection of sensitive data about minors and adults. A mandate to use such technologies could well do more harm than good.

AG Quotation in the Final Task Force Report: The Report includes a quotation from remarks that an Attorney General made to the Task Force about sex offenders on a social network. Although the Report briefly, and appropriately, explains why the AG's figures are not persuasive data, the assertions made warrant further analysis, which we provide at http://www.cdt.org/speech/CDT-ISTTFstatement.php.

For more information on CDT's views of the ISTTF Final Report, contact Leslie Harris at lharris@cdt.org or John Morris at jmorris@cdt.org, or at 202-637-9800.

December 17, 2008

Comcast: Statement Regarding the Internet Safety Technical Task Force's Final Report to the Attorneys General

Comcast is pleased to have had the opportunity to participate in the Internet Safety Technical Task Force. The company would like to thank the Berkman Center for Internet & Society at Harvard University for directing the Task Force, and recognize the efforts of its chair, Professor John Palfrey, the members of the Task Force's Technical Advisory Board and Research Advisory Board, as well as the other Task Force participants for their contributions to the Final Report.

The issue of online safety is complex, and the diversity of the Task Force participants themselves underscores how difficult it is to arrive at a consensus. Nevertheless, Comcast believes the Final Report to be significant contribution to the understanding of the dangers youth face in the current online environment, as well as the policy initiatives which are most likely to have a positive effect in promoting online safety.

Comcast commends the Task Force's compilation and review of the best available current academic research into how youth use communications technologies, and the resulting types of dangers that they face, and its use of this research as a basis for its policy recommendations. Comcast believes that policy decisions always benefit when they are informed by research and, given constantly changing nature of the online world, supports the Task Force's recommendation for more research in this field to deepen the understanding of the types of dangers youth may face online.

Comcast agrees with the Task Force that technology can enhance online safety and the company, like all major cable ISPs, provides its high-speed internet customers with free parental control software tools to help parents provide their children with age-appropriate Internet access, including technology for the filtering of offensive content, pictures and Web sites. Comcast agrees with the Task Force's recommendation that the development of online safety technologies benefits from collaboration between the Internet community and interested groups such as public policy advocates, social services, and law enforcement, and that these technologies should be informed by the current research regarding the types of risks minors face online.

However, as noted by the Task Force, the Internet itself, the ways in which minors use it, and the available technologies are constantly changing. As a result, Comcast further shares the Task Force's concern about an overreliance on technology in isolation or on a single technological approach.

Comcast also sees a significant role for education in enhancing online safety and provides its customers with significant online safety educational content, with sections for both parents and children, via the comprehensive Security Channel on our Comcast.net consumer portal (https://security.comcast.net).

ConnectSafely
Smart Socializing Starts Here™
www.connectsafely.org

Berkman Center for Internet & Society at Harvard University: Statement Regarding the Internet Safety Technical Task Force's Final Report to the Attorneys General

From: Larry Magid & Anne Collier, co-directors, ConnectSafely.org. December 17, 2008

Conventional wisdom and many of the technical products and services proposed to the Task Force point to greater parental control. The reasoning is that, if parents had the tools, resources and skills to control their children's Internet use, online youth would be safer. This is not an unreasonable approach but there are two potential problems with this assumption:

1) The research presented to the Task Force shows that greater parental control is not likely to be available to the children who are most at risk online. The highest-risk population does not enjoy the kind of parenting likely to adopt parental controls or opt-in programs.

2) A little-discussed additional risk: the unintended consequences of parental control. To explain:

There are parents who, for a variety of reasons (political, cultural, or religious beliefs, ignorance of the facts, fear of being exposed as abusers, etc.), would deliberately prevent their teens from accessing social-network sites (SNS). Parents do have rights regarding minor children, but children have rights as well, and taking away some of these could have a profound negative impact. A graphic example is the number of referrals directly from MySpace to the National Suicide Prevention Lifeline, which says peers are among the most important referrers of troubled teens. Other examples of unintended consequences:

- Teens who are abused, neglected or otherwise mistreated at home being denied access to a venue for discussing issues pertaining to their abuse, including how to find help.
- Teens seeking support when caught up in divorces or domestic conflict where the legal guardian wishes to "protect" them from their other parent.
- Teens losing access to resources that help them find their way out of eating disorders and other self-destructive behaviors.
- Gay and lesbian teens whose parents might prevent them from understanding their sexuality, possibly leading to further isolation, depression and self-destructive behavior.
- Teens who think they might have a STD being barred from getting help.
- Pregnant teens unable to explore their options.
- Law enforcement, social workers, and parents losing access to clues from youth who are using SNS to display their intentions to commit dangerous crimes.
- Parents, educators, and researchers losing access to unprecedented insights into adolescent development and behavior as well as self-destructive behavior.
- Children (including many who are U.S. citizens) being denied access because their parents are reluctant to fill out forms in fear of deportation or other legal consequences.
- Institutionalizing a youth culture of workarounds and deceit due to systemic restrictions.
- Creating for parents a false sense of "security" as new restrictions drive children underground to sites that are offshore or that simply aren't run by responsible companies.

We are concerned about any policy or technical control being imposed on youth Internet users without full consideration of these and other potential unintended consequences for youth whose parents are unable or unwilling to give their consent.

ENOUGH IS ENOUGH: STATEMENT REGARDING THE INTERNET SAFETY TECHNICAL TASK FORCE'S FINAL REPORT TO THE STATE ATTORNEYS GENERAL

The Internet has transformed from a collection of websites to a diverse communicative habitat. Although significant regions of this digital world are safe and well-lit, portions remain dangerous and "untamed". In this ever-evolving virtual space, the risks minors face are complex and multifaceted, and a combination of industry best practices, technologies, education efforts, parental involvement, law enforcement and policy solutions are needed to create and sustain a safe digital habitat for our children.

Significant strides have been made: The Internet industry, itself, has demonstrated substantial creativity, innovation and commitment to corporate responsibility. Social networking giants like MySpace proactively employ preventative and conscientious safety policies and technologies, but it is essential that successful best practices be adopted by the social networking industry-at-large for broader impact on youth safety. And, although challenges remain with respect to identity verification and authentication of minors online, of special note are findings by the TAB regarding new innovations in adult verification technologies, which could have significant implications "to reduce minors' access to adult-only sites"[1].

There is more work to be done: Further research is needed regarding pornography's impact on youth, specifically with respect to fueling youth risky behaviors including the sexual solicitation of other youth and adults online, and youth-generated child pornography. Additional research must also explore the impact of both legal and illegal online pornography on predators and in the sexual exploitation of children, as well as the role and impact of grooming in online victimization[2]. The preventative impact and critical need for aggressive enforcement of existing laws in the U.S. —specifically obscenity statutes—cannot be over emphasized.[3] Finally, the Task Force would have benefited from greater involvement from law enforcement officers, clinicians, psychologists, and parents to help paint a more holistic picture of Internet dangers and safety solutions.

Parents remain the first line of defense in protecting their children online: There is still no silver bullet to protect children online, and parents play a critical role, which is why our *Internet Safety 101: Empowering Parents Program* focuses on educating, equipping and empowering parents and other childcare givers to protect children through layered technical and non-technical measures.[4]

This report is an important step, but significant challenges remain We look forward to our continued work alongside the Attorneys General and other stake holders as we press on towards ensuring our children enjoy and safe, healthy and rewarding experience online.

Donna Rice Hughes, President, Enough Is Enough

---

[1] Enhancing Child Safety and Online Technologies: ISTTF Final Report: 29.
[2] Although the N-JOV study (Wolak et al. 2004) found that in Internet-initiated victimization deception was rare and youth willingly and knowingly met with their perpetrator, the role of grooming was not examined.
[3] Of youth who experienced unwanted exposure to online pornography, 57% encountered "people having sex" or violent or deviant images". (Online Victimization of Youth: Five Years Later. 2006).
[4] http://www.enough.org/inside.php?tag=internetsafety101

December 17, 2008

Family Online Safety Institute, Stephen Balkam, CEO: Statement Regarding the Internet Safety Technical Task Force's Final Report to the Attorneys General

We welcome the findings and recommendations of the Task Force's final report. Overall, it balances the need to respond to the broad range of issues that are of concern to the State AGs, while also being mindful of unintended consequences of mandating a particular technology solution.

I believe that Task Force carefully considered the problem posed to it, but also explored what existing and emerging research was saying about children and young teens actual experiences online. In this way, the Task Force moved the discussion from one that has been informed by fear and media overstatement, to one based on facts, statistics and descriptions of how kids are using the Internet.

While it became clear that there were a number of promising technological "solutions" – particularly when combined with each other – it also became clear that these technology fixes also came with public policy and social implications. It was remarked that both Germany and South Korea have national age verification and identity authentication methods employed in their countries, yet both depend upon national identity numbers being issued at birth – something that has been long resisted in the US.

An encouraging part of the Task Force deliberations was that no one in the group argued for or promoted the idea of a government mandate to use a particular technology or method to identify or verify a child's age. The consensus emerged that there needed to be a multi-stakeholder approach that emphasized some technology combined with adherence to sites terms of use together with much more comprehensive educational efforts. While this may appear to be a more complicated and onerous approach, no one advocated or identified a "silver bullet" that would address all of the concerns.

I would argue that this issue needs to be considered at the highest levels of government and that the new NTIA Working Group, created by Congress could productively address this at a national level. Further, more comparisons of international efforts would be beneficial. And, a storehouse or repository of good practice should emerge from the work of the Task Force to both gather all the excellent technology reviews and research papers that emerged, but also to be a growing and dynamic resource for all in the field of online safety.

IDOLOGY INC.

December 17, 2008 – IDology, Inc

Statement Regarding the Internet Safety Technical Task Force's Final Report to the Attorneys General

IDology, Inc finds issue with the final report and recommendations regarding the use of identity verification (IdV) and age verification solutions because:

- There are several technologies that exist that help keep kids safer when used in a layered approach and no substantive discussions were held on applying these together
- Policies of Social Networking Sites (SNS) rely on age and identity segmenting to protect minors and restrict content access as outlined in Appendix E of the report yet the verification processes are ineffective
- Terms of Service for most SNS require members to register with true and factual information about themselves making identity verification feasible
- Identity and age verification is commercially reasonable and being used today in numerous commercial applications including verification pursuant to government regulations
- The recommendations were developed around the perception that there is minimized risk to minors based on research; however, the scale of SNS is not taken into context so that even a small percentage of risk translates into millions of people
- The researchers admittedly report that there are limited numbers of large-scale studies and that there is no research regarding the online activities of registered sex offenders which was one of the major areas the Task Force was to study

Using IdV and age verification helps protect kids from 2 of the 3 threats the report outlines including sexual solicitation and access to problematic content. Overall IdV and age verification:

- Is commercially reasonable and verifies individuals 18+ that are legitimate identities
- Provides a higher knowledge based authentication method to verify someone is who they claim to be which is proven and effective today in helping businesses prevent fraud and identity theft in multiple industries
- Can help law enforcement locate an individual if there is inappropriate behavior from an adult toward a minor
- Separates adults from minors and prevents minors from accessing restricted content

Using IdV and age verification is a policy decision not a technology issue. The Task Force agrees that IdV is effective in certain environments; however it did not adequately discuss ways technologies and policies could be layered together and used to reduce risks to children. The Task Force does not provide best practices to solve the problem we were charged with examining and the report is based on limited research. The report criticizes effective technologies while promoting the initial steps SNS have taken. There is clearly much more work and vigorous discussion needed. For more information on IDology's position, visit http://blog.idology.com tag word MySpace or Internet Safety Technical Task Force.

iKeepSafe Statement Regarding the ISTTF Final Report to the Attorneys General

iKeepSafe would like to thank MySpace and the Attorneys General for convening the Task Force and providing the opportunity to review technology options for protecting youth online.

Age Verification

iKeepSafe carefully reviewed the proposals for technology solutions that would identify a parent-child relationship and age verification in an effort to reduce harmful contact and content. Some of the challenges to these technologies are:

a. We have no consistent and credible way to determine who is a ***custodial*** parent and who is a child. In today's Internet environment, this obstacle is insurmountable. (Would hospitals or county records clerks be asked to verify a birth parent? Is the birth parent still the legal guardian? Who determines eligibility? Will schools be asked to identify a custodial parent? Will a verification form, mailed or faxed from a residence determine parentage?)

b. Verifying children's ages will aggregate large databases of personal information of youth, creating problematic scenarios including commercial companies storing data on American children, identity risks, privacy concern, and substantial security risks. What happens when this database gets hacked?

c. It is important to note that many youth experience inappropriate contact and content, including home-produced pornography, *from other youth*. Age verification will not protect from these exposures.

Gaps in the Research

For those of us on the Task Force who produce prevention content, it was very helpful to have access to experienced researchers and quality research. Access to more comprehensive law enforcement data would have been helpful in giving a more complete view of problems youth face online. More statistics and research about what the states are experiencing in Internet crime units will help bridge the gap between what law enforcement is reporting to AGs and what we see in peer reviewed research. Additionally, many of the studies we reference were designed or rely on data that was gathered before 2006 when social networking exploded.

What Can Be Done Now

Because youth at risk (on and offline) are *not* likely to have parents engaged in their online safety, what can be done now to protect minors?

- Engage the public health community to develop and implement prevention, intervention, and bystander awareness initiatives.
- Invest in research to ensure that Internet safety and security efforts are targeted, relevant, and effective, including evaluations of existing safety content and programs.
- Increase post-conviction controls on convicted sex offenders and impose restrictions on the online activities of convicted child predators.
- Expand sex offender registry information to include Internet identifiers.
- Preserve Internet evidence for law enforcement investigations.
- Expand the reach and enforcement of child pornography reporting. Add state enforcement powers and broaden the scope of online companies that must report images of child pornography to the Cyber Tip Line at NCMEC (National Center for Missing & Exploited Children).
- Create a new crime of *Internet Sexual Exploitation of a Child*. Make it a crime to use a computer or computer network to encourage a child to engage in or to observe sexual activity while communicating online.
- Criminalize the luring of a child online. Make it a crime to use a computer or computer network to make sexually suggestive statements and to lure children into face-to-face meetings.
- Criminalize age misrepresentation with *Intent to Solicit a Child*. Make it a crime to lie about your age when enticing a child into criminal sexual conduct.
- Create incentives for law enforcement to make serving on cyber-crime units a career fast-track. Provide internal rewards and promotions. Hone technical skills and increase resources for officers and prosecutors.
- Educate children and parents. Provide school districts with online safety curricula for children and educational materials for parents teaching online security, safety, and ethics.
- Empower parents. Require Internet access providers to make filtering, blocking, and monitoring tools available.

Thank you for your consideration and your continued effort in our shared priority of protecting children online.

Marsali Hancock
President, Internet Keep Safe Coalition (www.iKeepSafe.org)

December 17, 2008

Adam Thierer, Progress & Freedom Foundation: Statement Regarding the Internet Safety Technical Task Force's Final Report to the Attorneys General

It has been a privilege to serve on the ISTTF. We have concluded there is no silver-bullet technical solution to online child safety concerns. This represents a major step forward. *Education and empowerment* are the most important parts of the solution. We can provide parents with more and better tools to make informed decisions about the media in their children's lives. But technology can only supplement—it can never supplant—education and mentoring. If the ISTTF had one failing, however, it was that we did not go far enough in illustrating why mandatory age verification (AV) will not work and would actually make kids *less* safe online. It is unwise for lawmakers to require that even more personal information (about kids, no less) be put online at a time when identity theft continues to be a major problem. Moreover, because it will not work as billed, AV would create a false sense of online security for parents and kids alike. Enforcing such mandates may also divert resources that could be better used to focus on education and awareness-building efforts, especially K-12 online safety and media literacy education. To the extent some policymakers persist in this pursuit of a technological Holy Grail, they must address the following five problems with mandatory age verification regulation:

1) **The Risk Mismatch Problem**: The ISTTF has shown that the primary online safety issue today is peer-on-peer cyber-harassment, not adult predation. Mandatory AV would do nothing to stop cyberbullying. Indeed, the lack of adult supervision may even exacerbate the problem.

2) **The Non-Commercial Speech Problem**: AV schemes *may* work for *some* commercial websites where transactions require the transfer of funds, goods, or services. AV may also work in those contexts (i.e., online dating services) where users *want* to be verified so others know more about them. But most social networking sites (SNS) are non-commercial and users do not want to divulge too much personal information. This will significantly complicate AV efforts.

3) **The Identity Matching Problem**: Because little data exists to verify minors, AV won't work for sites where adults and minors coexist, or to keep adults out of "child-only" sites. Parental permission-based systems have similar shortcomings. If the parent-child relationship cannot be definitively established, fraud is possible. Even if we solve the initial enrollment problem, how do we prevent children from later sharing or selling their credentials to others? How do we prevent older siblings from sharing their credentials with younger siblings? How do we prevent predators with children from using their child's credentials to gain access to a child-only SNS?

4) **The Scale / Scope Problem**: How broadly will "social networking sites" be defined? Will hobbyist sites, instant messaging, video sharing sites, online marketplaces, or online multiplayer gaming qualify as SNS? Can we expect *every* parent to go through the steps necessary to "verify" their kids for everything defined as a SNS? How burdensome will authentication mandates be for smaller sites? Will the barriers to site enrollment force previously free SNS to begin charging fees? Importantly, forcing schools into the AV process will impose significant burdens (and potential liability) on them. Finally, how well would mandatory AV work for a global platform like the Internet? Even if domestic SNS don't flee, many users *will* likely seek out offshore sites to evade domestic regulations. Those offshore sites are often not as accountable to users or law enforcement as domestic sites, creating new risks.

5) **The Speech & Privacy Problems**: Are we restricting the speech rights of minors by making it so difficult for them to communicate with others in online communities? Regarding privacy, many parents, like me, encourage their kids to put *zero* information about themselves online because we believe that will keep them safer. AV mandates are at cross-purposes with that goal.

December 17, 2008

As a continuation of our very productive work with the Attorneys General over the past three years, Facebook is proud to have been part of the Internet Safety Technical Task Force. We have been particularly glad to have the opportunity to highlight our extensive technology design and rules around identity and personal interaction that are contributing to making the Internet more safe and trusted.

Since our founding in a Harvard dormitory in 2004, Facebook has believed that making the world more open and connected works hand-in-hand with making it safer and more secure.

In addressing the threats and potential threats that minors face, we have deployed privacy rules that limit the availability of information by default, content and account access rules that require users to take responsibility for their behavior, technologies that capture and react to anomalous behavior, and an extensive reporting infrastructure backed up by well-trained user operations "cops on the beat." When inappropriate behavior turns into illegal behavior – in any community of over 140 million people, there will inevitably be attempts at crime – we work closely with law enforcement to bring the perpetrators to justice.

Facebook's safety and security design is constantly evolving and improving to address threats as they arise, and both the Attorneys General and the Task Force are playing key roles in informing our dedication of resources to addressing safety and security threats, especially those involving minors.

Protecting minors from harm is a shared responsibility among online sites, parents, teachers, children themselves, researchers and education organizations, and law enforcement. We at Facebook look forward to continuing our diligent work with all of these stakeholders to build a safer Internet.

--Chris Kelly, Chief Privacy Officer

facebook

Address: 156 University Avenue
Palo Alto, CA 94301
Telephone: 650.543.4800
Fax: 650.543.4801

Linden Lab®

Statement of Linden Lab Regarding the Internet Safety
Technical Task Force's Final Report to the Attorneys General

It has been a privilege for Linden Lab, operators of the Second Life "virtual world," to participate in this mission-critical Task Force. We applaud the Attorneys General for shedding light on the potential risks our children face online. We likewise applaud fellow Task Force and Technical Advisory Board members who devoted great human capital and resources to this effort, sharing a wide array of solutions, experiences, and knowledge. We especially thank John Palfrey, danah boyd, Dena Sacco, and the Berkman Center for rising to a Herculean challenge – leading us in evaluating, explaining and categorizing with substance and precision the risks at hand, and setting out how our industry may – and must – work to mitigate these risks.

Virtual worlds like Second Life have often been referred to as the "Next Big Thing" on the Internet. Hundreds of universities, charities, retailers and other organizations now use Second Life to increase productivity, drive collaboration, and increase their visibility and outreach. Clearly, virtual worlds hold great promise for America, our economic development, and our ability to compete globally. They mark a leap forward in how we can learn and work together over geographic distances. Thousands of adults and children have learned important graphic, coding and scripting skills from our platform, whether working with schools, universities and non-profits, or independently.

It is critical that Second Life and the entire virtual worlds industry provide these opportunities to our youth in a safe and secure environment. Linden Lab thus has been proactive about child safety – taking a holistic approach to designing our platform with safety in mind. The Second Life grid (web entry point secondlife.com), for instance, is not currently marketed to or intended for minors. When reported or discovered, minors are removed and banned. But we know teenagers are interested in virtual worlds, so in 2005 we created a separate, secure environment for teen residents called Teen Second Life, or TSL (teen.secondlife.com). Teens 13-17 may set up TSL accounts to create, collaborate and learn. With the exception of Linden Lab staff (who are available to help) and educators (who undergo a background check), no adults are permitted to interact with these users.

While most teens seem to prefer TSL, we also know that some may (despite our prohibition) access Second Life. However, we believe it is important that these teens be blocked from "adult" content or discussions. Thus, we provide at no charge an age verification solution (through Aristotle) for all "landowners" to whom we lease Second Life server space. We ask these content providers to activate this age verification solution if they conduct adult-oriented discussions or provide adult content, in particular of a sexual nature. We are currently evaluating how to make wider use of our age verification solution.

We are proud that a wide range of users with varied interests – adults and teens – employ our platform to learn, collaborate and grow. We are very proud that there has never (to our knowledge) been a single incident of child predation arising from Second Life. And as our community and our services expand, we will always focus deeply and broadly on how technology and platform design can continue to ensure that kids enjoy and learn how to use virtual words, while in a safe and secure environment.

December X, 2008

Berkman Center for Internet & Society at Harvard University: Statement Regarding the Internet Safety Technical Task Force's Final Report to the Attorneys General

Microsoft greatly appreciates the work and dedication, from a broad cross section of industry, civil society, and the academy, that went into this report. We think the report is, as it notes, a set of guideposts for next steps, but not final answers. In that light, we are eager to work with the Attorneys General and others to help carry this work forward.

Microsoft believes that the Task Force report largely speaks for itself, but we write separately to emphasize two points: first, we think it is critical that the online safety issues identified here – in particular, the age and identity verification questions that animated the creation of this Task Force – are understood in their larger context. Second, we do not want our articulation of either our belief that the Internet is at an important moment regarding identity and authentication, or our description of technologies for more secure identity and authentication, to be misinterpreted or misused in policy debates.

As Microsoft identity strategist Kim Cameron wrote in early 2006, "*The Internet was built without a way to know who and what you are connecting to. This limits what we can do with it and exposes us to growing dangers. If we do nothing, we will face rapidly proliferating episodes of theft and deception that will cumulatively erode public trust in the Internet*." From our perspective, the risks of doing nothing include both threats to public trust, privacy and security, but also the possibility of more draconian responses which would unduly restrict important social values like anonymity and privacy.

Since that time, Microsoft has developed a series of observations regarding this problem, including the Laws of Identity, the Identity Metasystem, and more recently, End to End Trust, as well as contributing to the development of more secure forms of authentication – in particular Information Cards. These ideas have been, and continue to be, refined through blog commentary, industry and academic discussions, and practical analysis across a wide variety of privacy, security, cybercrime, and online safety issues.

These ideas are germane here in two respects. First, the Task Force report is absolutely correct that in working towards solutions, the Internet community should give appropriate care to the privacy and security of user information, especially information on minors. Second, the Task Force report identifies correctly that no single technology can solve online safety risks, and that there are important policy choices associated with how we move forward. We do not believe, however, that the need to address these choices means we should not pursue options for greater trust online.

In order that our views on some of these policy issues were not misunderstood, we wrote directly to Attorneys General Blumenthal and Cooper to express our support for their work, and to make plain our positions on policy issues, including those related to regulation, anonymity, privacy and human rights. A copy of that letter is available on our End to End Trust website through the link here. We look forward to the work ahead.

myspace.com
a place for friends

MYSPACE: IN SUPPORT OF THE INTERNET SAFETY TECHNICAL TASK FORCE'S FINAL REPORT TO THE STATE ATTORNEYS GENERAL

At MySpace the safety of our users is a top priority, and we congratulate the Berkman Center for creating a well-grounded process that allowed this multi-dimensional Internet Safety Technical Task Force to tackle the challenge of identifying technologies that effectively improve online safety for our nation's youth. MySpace also thanks Attorneys General Richard Blumenthal and Roy Cooper for their leadership in online safety and for working collaboratively to identify effective Internet safety solutions.

The Final Report highlights the many challenges that must be understood and overcome in order to determine which solutions best improve online safety for youth. In the end, any solutions implemented must be comprehensive. The Report recognizes that while technology has a role to play, it must be integrated into a larger set of solutions that includes all societal sectors that have a stake in protecting our children online, including industry, policy makers, law enforcement, educators, parents, healthcare professionals and non-profit organizations. The Final Report makes key findings and recommendations with these considerations in mind – an approach we fully support that reflects our own approach to online safety.

MySpace's submission to the ISTTF highlights our holistic approach to safety, security and privacy. Our program integrates technological, educational, enforcement, policy, and collaborative solutions into the online environment that our teens traverse daily. Over the last two years, we implemented over 100 safety innovations by working with our partners in the law and policy-maker, NGO, industry, parent, teacher and law enforcement communities. We started a paradigm shift away from the notice and takedown only regime to one that proactively identifies challenges and solutions around the three 'C's'. Through this new regime we focus on reducing unwanted Contact and access to inappropriate Content, and we find ways to Collaborate with our partners and educate our stakeholders, including parents, teens and educators.

Our submission points out that online sites should engage in at least the following "Big Six" safety practices, which are fundamental parts of the MySpace safety and security program: (1) Review images and video for inappropriate content; (2) Check discussion groups and remove illegal or harmful content; (3) Remove registered sex offenders using the most rigorous currently available technology; (4) Enforce minimum age requirements using cookies and search algorithms; (5) Protect younger users from adults they don't already know in the physical world through default privacy settings and other knowledge-based site features; and (6) collaborate with law enforcement and online safety advocates to provide 24/7 response for any issues and to raise awareness and education related to online safety.

This unprecedented Task Force was given the challenging mandate of determining the extent to which today's technologies could help address online safety risks faced by young Internet users. MySpace fully supports the findings of the Research Advisory Board in recognizing that at-risk teens in the physical world are the most at-risk online, and that much work needs to be done to identify and address the needs of these teens. Although not all technologies presented to the Technical Advisory Board were applicable to overcoming the risks teens face online, MySpace finds promise in many of technologies reviewed. The 17 recommendations of the Task Force correctly constitute a call to action for industry, researchers, healthcare professionals, technologists, law enforcement, law makers, educators and parents – all of whom are stakeholders in protecting our children online.

We look forward to continued collaboration with members of the Task Force. Online safety for us is a journey, not a destination. Using the recommendations in the Final Report, we begin now the next phase of our ongoing journey to provide a safer online experience for all of our users.

Hemanshu Nigam, Chief Security Officer, MySpace

###

December 17, 2008

December 17, 2008

Institute for Policy Innovation: Statement Regarding the Internet Safety Technical Task Force's Final Report to the Attorneys General

The Institute for Policy Innovation (IPI) is a free market-oriented public policy think tank. IPI has been involved for many years with Internet and communications policy, including efforts to make children safer online. IPI certainly appreciated the opportunity to serve on this Taskforce and be part of this important work.

We have found that where government at all levels—federal, state, local or other political subdivision—has avoided layering in new regulation that a discernable benefit to the technology marketplace has continued. Largely because innovation so rapidly outpaces legislation or regulation they simply are not an effective means of problem solving, or worse, they freeze innovation and therefore the related economy. More specifically these actions lead to an increase consumer choice and enhanced services.

In fact, the case is made again with respect to social networking sites (SNS). As noted in the report, "…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 failsafe."

Importantly, as the above makes clear, law enforcement has a critical role in the mission to protect our children, but that role is not in mandating technologies. As is made clear in the report, technology mandates do not work. At best they are obsolete within days, and at worse are harmful often because of the false sense of security they inspire. As expressed in the report, the right answer is much harder and therefore deserves that much more attention, "Instead, a combination of technologies in concert with parental oversight, education, social services, law enforcement, and sound policies by social network sites."

The truth is that there is no "Internet safety" there is simply "safety," and so all of the concerns raised are social issues which extend beyond the scope of the Internet, much less SNS. That is why law enforcement has a critical role to play in making priority the most likely threats (such as bullying), educating the public about these threats, stopping the "bad guys," and not sensationalizing the Internet challenges.

IPI is prepared to assist the attorneys general, the governors, and the state and federal legislators in addressing these issues and look forward to doing so.

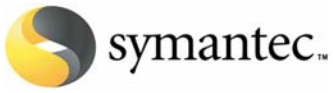
December 17, 2008

Sentinel Tech Holding Corp.: Statement Regarding the Internet Safety Technical Task Force's Final Report to the Attorneys General

Sentinel would first like to thank the Berkman Center for a job very well done. We would also like to thank the Attorneys General and MySpace for creating and convening this taskforce. Lastly, we would like to thank the members, the Research Advisory Board, and the Technical Advisory Board for all of the hard work and thoughtful consideration

We are pleased that the Task Force came to a conclusion that we as a company, and many in our industry came to several years ago. Age/identity verification/authentication is a non solution as it pertains to the online social networking industry or any other online entities where minors interact with adults. We have long believed that the risks were great, and there were no rewards. These services are among our product offerings, but we made a decision not to sell them to sites that catered to minors, or sites where minors and adults could interact. Our decision was based on our commitment to good corporate citizenry and best business practices. Even though the decision cost us money, we now know it was the right one as an independent and esteemed group of industry, policy, and academic professionals have validated our actions.

While the Task Force found age verification ineffective, we are encouraged by, and better educated as a result of, the in depth analyses of other technologies. Learning the pros and cons of a wide variety of offerings makes us a stronger industry, and gives us guidance as we embark upon a new year of research and development.



December 17, 2008

Marian Merritt, Internet Safety Advocate, Symantec
Statement Regarding the Internet Safety Technical Task Force's Final Report to the Attorneys General

Symantec supports many of the recommendations made by the ISTTF to the country's attorneys general with regards to promoting online safety for children. The report underscores the fact that ensuring online safety for children goes beyond deploying technology. No matter what laws are passed or what software is used, online safety for children still boils down to good parenting. The report also emphasizes that parents need to be proactive in communicating with their children about how to stay safe online and be good cyber citizens, just as they would teach them about safe and good behavior in the real world. Parents need to be involved in their kids' online world by educating themselves about the dangers and having regular conversations with their kids about their online activities.

Symantec also endorses the idea that technology should not be mandated. Addressing online child safety goes beyond the scope of what technology alone can do. It would be disingenuous and dangerous to instill a false sense of security among parents that they can install software and be satisfied that their children are protected. A parent cannot download software programs into a computer and expect that their work is done. Filtering and monitoring technologies are an essential element of child online safety, but only when they are coupled with the active involvement and participation of parents and schools to configure the software correctly, update that software, and carefully monitor the Web sites children are accessing.

Mandating age verification technology – particularly for social networking sites – is not a workable solution at this time to ensure child online safety. It is too easy to subvert such technology and imposing a specific solution would imbue a false sense of security for all involved that actually will result in more danger than safety. Instead, we advocate that attorneys generals and other government officials take the lead in pushing for legislation to establish child online safety curriculum requirements at the K through 12 level that contain what Symantec and the National Cyber Security Alliance call the Three C's: Cyber Safety Best Practices, Cyber Security Best Practices, and Cyber Ethics. First we need to help children understand why they shouldn't disclose their personal information, to keep away from strangers online, and to communicate with parents and teachers if they see something online that alarms them. Second, we need children to understand the basics of firewalls, antispyware and antivirus technology so they will think to make sure all are in place before surfing the Web. Finally, we must teach children that even though they're online, it's still wrong to steal, snoop, and bully just as it is wrong to do that in everyday life.

December 17, 2008

Verizon Statement Regarding the Internet Safety Technical Task Force's Final Report to the Attorneys General

Verizon commends the Berkman Center for the high quality of its report of the Internet Safety Technical Task Force. We applaud the good work and research in the report and agree with most of the recommendations, with the notable exception of Section VII.B, which we believe has the potential to significantly increase individual and corporate taxes. That said, we think there are some additional points Attorneys General, legislators, and regulators need to consider vis-à-vis online safety:

- **Regulation would diminish, not improve, internet safety.** The internet is a global network of networks -- about 25,000 interconnected networks make up the public internet. These networks are owned and operated by corporations, governments, schools, and not-for-profits. Local attempts to regulate the global internet are an exercise in futility: "The internet treats regulation as a failure and routes around the problem." (Larry Downes, cNET)

- **Considerably more work is needed before age verification will be viable.** While age verification software works for adults, verifying the age of as minor is an entirely different class of problem with no ready technical fix, i.e., there is no "silver bullet." It is not feasible to merely port an adult solution into the kids' domain. Besides creating a false sense of security for parents and kids, some of the software presented would actually create "honey pots" – databases full of information about kids – and as we all know, no online database is entirely hacker-proof. Another proposal would put the burden on schools to maintain these databases, something the schools have neither the expertise nor the resources to carry out safely and securely.

- **Verizon commends MySpace and FaceBook** for the steps they've taken this year to make their sites safer for everyone. The actions of these two companies should serve as a model for other social networking sites.

Verizon takes our responsibility to protect our customers very seriously. We look forward to working with our industry partners to make the internet a safer place for teens, and increasingly, seniors, in a cooperative and collaborative fashion. Likewise, we hope the Attorneys General, on the front lines of law enforcement, continue their active dialog with industry and child protection groups.

WiredSafety's Statement Regarding the Internet Safety Technical Task Force's Final Report to the Attorneys General December 17, 2008
Due to space limitations, www.wiredsafety.org/taskforce contains supplemental information to this comment incorporated by reference herein, updated as needed. Our appreciation, especially to the Attorneys General, is set forth therein.

WiredSafety is a grass-roots all-volunteer charity that helps empower Internet users of all ages and addresses risks encountered online and on mobile, cell and gaming devices. It first began operations in 1995 and is run by Parry Aftab, an Internet privacy and security lawyer (also an unpaid volunteer), WiredSafety is best known for its unique insight into how young people use technologies, identifying the risks they face and framing solutions to those risks.

It does this by engaging teens and preteens in the process. Teenangels, and its younger counterpart, Tweenangels, are WiredSafety's youth cybersafety leadership and research programs. They don't just learn about cybersafety, they teach others, research the issues and create solutions and awareness programs of their own. The Teenangels advise industry, appear on TV, testify before Congress, conduct presentations, publish research and host summits.

While we agree with the ISTTF Report as a whole, we have some concerns over the shortage of current and relevant research which can lead to out-of-date and, in some cases, misleading conclusions. The Teenangels research is designed to elicit relevant information about what teens and preteens do online and how this information can be used to forge awareness, education, technology and policy solutions. And because teens are more frank with their peers than adults whom they fear may tell their parents, these findings are compelling, insightful and meaningful.

In a survey of 512 7^{th} – 12^{th} grade girls, 44% said they were cyberbullied, most from their best friend (19%), boyfriend or girlfriend (9%) or an acquaintance (57%). More than 60% shared their passwords with others. (There is a direct connection between misuse of passwords and cyberbullying.) Younger teen girls take more risks than older ones (19% of one poll admitted to a real life meeting with someone that they had only known online. Most of these were freshmen girls.) In the same survey, 10% of the students had between 10 and 50 strangers on their social networking "friends" list. 75% had 100 or more friends on their "friends list (50% had 200 or more). Teen girls believe that they are safe online, but their friends are not. (89% felt they were safe online, but thought 28% of their friends were unsafe online.) 96% of the teen girls polled had a social networking profile. Given the kinds of things they chose as passwords, 91% of their passwords can be easily guessed by others in their class. Password abuse is the root of much evil.

How do girls and boys compare? In a separate study of 547 boys and girls, boys were almost twice as likely to share their cell numbers on their profiles. A review of these findings disclosed that boys tend to feel safer and therefore share more contact information online than girls.

While not classified as "peer-reviewed," teen peer-conducted surveys provide fresh, relevant and much needed information about young people online. As we search for answers, young people must be part of the process, the research and in framing solutions and meaningful approaches. (For more research results, our full comments and our appreciation to all involved for their extraordinary effort and the honor of being a part of the ISTTF, visit wiredsafety.org/taskforce.)

December 17, 2008

Yahoo! Statement Regarding the Internet Safety Technical Task Force's Final Report to the Attorneys General

Yahoo! wishes to thank the Attorneys General, Berkman staff, and the task force participants for their hard work in developing a report that clarifies the risks currently facing children, and sheds light on the efficacy of existing technologies. We look forward to continuing our work with the state Attorneys Generals, policymakers and industry colleagues on developing an online environment that protects children and fosters innovation and learning.

As we noted in our previous submission, Yahoo! has been a leader in keeping kids safe online through a variety of technical and non-technical means: our "Report Abuse" functionality, which is included on various sites across our network, allows us to more effectively address distribution of illegal content or occasions of harassment or cyberbullying; "Safe Search" allows parents to shield their children from unwanted exposure to adult content; built-in privacy features give users the ability to control who can contact them using such services such as Yahoo! Messenger, Answers and Profiles; and Yahoo! has implemented technology and policies to help us identify and remove apparent child pornography violations on our networks. Yahoo! also provides parental controls to our users through our broadband access partners such as Verizon or AT&T.

In addition, we partner closely with public safety officials to improve the safety of our sites and services. We have a dedicated compliance team that can immediately respond to law enforcement if we are contacted about a situation that indicates a child may be in danger. Yahoo! also dedicates employees to provide law enforcement training for the members of the Internet Crimes Against Children Task Force, state Attorneys General, the National Association of Attorneys General and others. We have held law enforcement training seminars in conjunction with the Attorneys General of Colorado, New Jersey, Illinois, Texas, Missouri, New York and Nebraska.

As such, it should be clear that online safety is a multi-faceted challenge whose success requires close cooperation between the private and public sector. But success also requires the enactment of policies that strengthen the hand of law enforcement by providing law enforcement agencies the tools and resources they need to identify, prosecute and incarcerate those who would prey on children, such as recidivist sex offenders. Similarly, success requires the enactment of policies that assure the public that once those criminals (who have an extremely high rate of recidivism) are incarcerated, they will not shortly be back on the streets to reoffend.

We think collaboration with organizations such as this task force is critical for identifying and implementing solutions that create real progress on this complex and challenging issue.