



Health Information Privacy: Current Trends, Future Opportunities

March 17, 2010

CDT is a non-profit public interest organization founded in 1994 and dedicated to keeping the Internet open, innovative and free. With offices in Washington, DC and San Francisco, CDT works with all interested stakeholders to develop and advance public policies, corporate practices and technology designs that enhance free expression, privacy, and democratic participation. Through research, dialogue, and advocacy, CDT's Health Privacy Project is promoting pragmatic, effective actions to better protect the privacy and security of electronic health information and build consumer trust in a wired health care system, so that the benefits of health information technology can be realized. CDT's work on consumer privacy on the Internet focuses on protecting the privacy of consumer's health information on-line, as consumers increasingly use the Internet to access and share health information on-line. This FTC roundtable touches on CDT's work in these areas.

Thank you for the opportunity to submit these comments to the Third Roundtable on Privacy. Those expressed here focus on protections for health information as part of electronic medical records kept by traditional participants in the health care system (such as physicians and other care providers, hospitals, and health plans), and personal health records, which are commonly offered by Internet companies and allow consumers to store and share copies of their health information with their health care providers and others as they see fit. We also briefly address FTC's specific question for this Roundtable on different standards for minors. CDT also is separately submitting comments for this Roundtable on identity management and submitted comments for previous Roundtables on on-line privacy with respect to sensitive personal information, including health.

Privacy and Security Protections Are Critical to Achieving the Benefits of Health IT

Health information technology (health IT) and electronic health information exchange have the potential to improve health care quality and efficiency, while also empowering consumers to play a greater role in their own care. Survey data shows that Americans are well aware of and eager to reap the benefits of health IT. A large majority of the public wants electronic access to their personal health information – both for themselves and for their health care providers – because they believe such access is likely to increase their quality of care.

At the same time, however, people have significant concerns about the privacy of their medical records, posing the risk that people will not trust, and therefore will not use, electronic health records systems if they do not protect privacy and security. In a national survey conducted in 2005, 67% of respondents were "somewhat" or "very concerned" about the privacy of their personal medical records.¹ In a 2006 survey, when Americans were asked about online health information:

¹ National Consumer Health Privacy Survey 2005, California HealthCare Foundation (November 2005) (2005 National Consumer Survey).

- 80% said they are very concerned about identity theft or fraud;
- 77% reported being very concerned about their medical information being used for marketing purposes;
- 56% were concerned about employers having access to their health information; and
- 55% were concerned about insurers gaining access to this information.²

These concerns are well founded. As the repeated reports of both small-scale browsing and large-scale breaches demonstrate, serious vulnerabilities exist now and could grow with the increasing flow of data. With computerization, tens or hundreds of thousands of health records can be accessed or disclosed through a single breach.

Protecting privacy is important not just to avoid harm, but because good healthcare depends on accurate and reliable information.³ Without appropriate protections for privacy and security in the healthcare system, patients will withhold information from their health providers due to worries about how the medical data might be disclosed.⁴ According to a recent poll, one in six adults (17%) – representing 38 million persons – say they engage in “privacy-protective” behaviors to avoid having their personal health information used inappropriately.⁵ Persons who report that they are in fair or poor health and racial and ethnic minorities report even higher levels of concern about the privacy of their personal medical records and are more likely than average to practice privacy-protective behaviors.⁶

The consequences of this climate of distrust are significant – for the individual, for the medical community, and for public health:

- The quality of care these patients receive may suffer;
- Their willingness to access health information on-line and seek support from social networking sites will be diminished;
- Their health care providers’ ability to diagnose and treat them accurately may be impaired;
- The cost of care escalates as conditions are treated at a more advanced stage and in some cases may spread to others; and
- Research, public health, and quality initiatives may be undermined, as the data in patient medical records is incomplete or inaccurate.⁷

These concerns must be addressed – and it is possible to do so. Privacy and security should not be an impediment to adoption of health IT. To the contrary, sound privacy and security policies, implemented in law, corporate practice and technology design, can enable health IT. Indeed, electronic systems, properly designed and managed, have a greater capacity to protect personal health information than is the case now with paper records. Digital technologies, including strong user authentication and audit trails, can be employed to limit and track access to electronic health information automatically.

² Study by Lake Research Partners and American Viewpoint, conducted by the Markle Foundation (November 2006) (2006 Markle Foundation Survey).

³ See Janlori Goldman, “Protecting Privacy to Improve Health Care,” Health Affairs (Nov-Dec, 1998) (Protecting Privacy); Promoting Health/Protecting Privacy: A Primer, California Healthcare Foundation and Consumers Union (January 1999), <http://www.chcf.org/topics/view.cfm?itemID=12502> (Promoting Health/Protecting Privacy).

⁴ Protecting Privacy; Promoting Health/Protecting Privacy; 2005 National Consumer Survey.

⁵ Harris Interactive Poll #27, March 2007.

⁶ 2005 National Consumer Survey.

⁷ Id.

Electronic health information networks can be designed to facilitate data sharing for appropriate purposes without needing to create large, centralized databases that can be vulnerable to security breaches. Encryption can help ensure that sensitive data is not accessed when a system has been breached. Privacy and security practices are not 100% foolproof, but the virtual locks and data management tools made possible by technology can make it more difficult for bad actors to access health information and can help ensure that, when there is abuse, the perpetrators will be detected and punished.⁸

The American Recovery and Reinvestment Act of 2009 (ARRA)⁹ included a number of improvements to federal health information privacy rules promulgated under the Health Insurance Portability and Accountability Act (HIPAA), many of which had been recommended by CDT.¹⁰ However, these provisions present numerous implementation challenges, and gaps in protections remain to be filled. Current policies still fall short of the comprehensive framework of privacy and security protections that will enable us to realize the tremendous potential of health IT. These comments touch on some of the critical work that lies ahead

We do need to act with some urgency. Privacy experts widely agree that it is often difficult or impossible to establish effective privacy protections retroactively. Restoring public trust that has been significantly undermined is much more difficult than building it at the start. Now—in the early stages of health IT adoption—is the critical window for addressing privacy. CDT and others call this “privacy by design.”

A Basic Question: What Is Privacy?

A comprehensive privacy and security framework for health IT will --

- Implement core privacy principles;
- Adopt trusted network design characteristics; and
- Establish oversight and accountability mechanisms.

What do we mean by “core privacy principles?” Although privacy is one of the most deeply cherished of rights, it is also one of the most misunderstood concepts. We use the word “privacy” to mean many things, ranging from communications privacy (such as the privacy of email or telephone calls) to privacy in the context of intimacy, sexuality and the family. The specific aspect of privacy that is at issue in the health IT debate is “information privacy,” which focuses on how information is used to provide a service to people or to make decisions about them. The concept of information privacy goes well beyond what is kept secret or hidden. After all, even without health IT, medical information flows from doctor to nurse to office administrator to pharmacy to insurance company to public health authority. The modern healthcare system is a complex ecosystem with many entities requiring access to health data to deliver and pay for care. Even with the most rudimentary technology, information is copied, shared and used for a variety of purposes that go beyond treatment and payment. Health privacy must account for all these uses. Therefore health privacy, comprehensively conceived, would provide a set of rules for who gets access to what information, under what conditions, and for what purposes.

⁸ See For The Record: Protecting Electronic Health Information, Committee on Maintaining Privacy and Security in Health Care Applications of the National Information Infrastructure, Computer Science and Telecommunications Board, National Research Council (National Academy Press, Washington, DC 1997) for a discussion of the inability of systems to be 100% tamperproof.

⁹ Public Law 111-5 (referred to herein as ARRA).

¹⁰ For a summary of the privacy provisions in ARRA, see http://www.cdt.org/healthprivacy/20090324_ARRAPrivacy.pdf.

This concept of privacy is sometimes referred to as “fair information practices,” a term that conveys the notion that data will be used and exchanged but must be handled by all parties in a way that is fair to the individual. While there is no single official formulation of the fair information practice principles, the Markle Foundation’s multi-stakeholder Connecting for Health initiative¹¹ outlined them as follows:

- **Openness and Transparency:** There should be a general policy of openness about developments, practices, and policies with respect to personal data. Individuals should be able to know what information exists about them, the purpose of its use, who can access and use it, and where it resides.
- **Purpose Specification and Minimization:** The purposes for which personal data is collected should be specified at the time of collection, and the subsequent use should be limited to those purposes or others that are specified on each occasion of change of purpose.
- **Collection Limitation:** Personal health information should only be collected for specified purposes, should be obtained by lawful and fair means and, where possible, with the knowledge or consent of the data subject.
- **Use Limitation:** Personal data should not be disclosed, made available, or otherwise used for purposes other than those specified.
- **Individual Participation and Control:**
 - Individuals should control access to their personal health information:
 - Individuals should be able to obtain from each entity that controls personal health data, information about whether or not the entity has data relating to them.
 - Individuals should have the right to:
 - Have personal data relating to them communicated within a reasonable time (at an affordable change, if any), and in a form that is readily understandable;
 - Be given reasons if a request (as described above) is denied, and to be able to challenge such a denial;
 - Challenge data relating to them and have it rectified, completed, or amended.
- **Data Integrity and Quality:** All personal data collected should be relevant to the purposes for which they are to be used and should be accurate, complete and current.
- **Security Safeguards and Controls:** Personal data should be protected by reasonable security safeguards against such risks as loss, unauthorized access, destruction, use, modification or disclosure.
- **Accountability and Oversight:** Entities in control of personal health data must be held accountable for implementing these information practices.

¹¹ See www.connectingforhealth.org for a more detailed description of the Markle Common Framework.

- **Remedies:** Legal and financial remedies must exist to address any security breaches or privacy violations.¹²

The federal HIPAA privacy and security regulations include provisions that address to some degree many of these principles. As noted above, the privacy provisions in ARRA made major improvements – but significant gaps remain, and effective implementation of will require major effort. These comments focus on establishing privacy protections for personal health records, which are largely offered by entities outside the traditional medical system. The comments also address a number of key issues that arise with respect to access, use and disclosure of health information by health system participants, including: downstream data uses; new health information exchange networks; data that qualifies as de-identified under HIPAA; stronger implementation of collection limitations through the minimum necessary standard; and tighter rules on use of data for marketing. The comments also briefly address standards for minors' information.

Establishing Privacy Protections for Personal Health Records

To keep pace with changes in technology and business models, additional legal protections are needed to reach new actors in the e-health environment and address the increased migration of personal health information out of the traditional medical system. Personal health records (PHRs) and other similar consumer access services and tools now being created by Internet companies such as Google and Microsoft, as well as by employers, are not covered by the HIPAA regulations unless they are being offered to consumers by covered entities.¹³ In the absence of regulation, consumer privacy is protected only by the PHR offeror's privacy and security policies (and potentially under certain state laws that apply to uses and disclosures of certain types of health information). If these policies are violated, the FTC may bring an action against a company for failure to abide by its privacy policies. The policies of PHR vendors range from very good to seriously deficient.¹⁴

The absence of any clear limits on how these entities can access, use and disclose information is alarming – and has motivated some to suggest extending HIPAA to cover PHRs. However, CDT has cautioned against this one-size-fits-all approach. The HIPAA regulations set the parameters for use of information by traditional health care entities and therefore permit access to and disclosure of personal health information without patient consent in a wide range of circumstances. As a result, it would not provide adequate protection for PHRs, where consumers should be in more control of their records, and may do more harm than good. Further, it may not be appropriate for HHS, which has no experience regulating entities outside of the health care arena, to take the lead in enforcing consumer rights and protections with respect to PHRs.

¹² In comments submitted by CDT to the FTC in November 2009, we urged FTC to adopt an updated, comprehensive set of FIPs for Internet privacy based on those more recently issued by the Department of Homeland Security. See http://www.cdt.org/privacy/20091105_ftc_priv_comments.pdf. The Markle Connecting for Health framework was largely designed to apply to patients and health care industry management of health information, but the FIPs in both the Markle and DHS models are similar.

¹³ HIPAA applies only to covered entities – providers, health plans, and health care clearinghouses. Section 1172 of the Social Security Act; 45 CFR 164.104. As explained in more detail below, ARRA extended the reach of some of HIPAA's regulations to business associates, which receive health information from covered entities in order to perform functions or services on their behalf.

¹⁴ The HHS Office of the National Coordinator commissioned a study in early 2007 of the policies of over 30 PHR vendors and found that none covered all of the typical criteria found in privacy policy. For example, only two policies described what would happen to the data if the vendor were sold or went out of business, and only one had a policy with respect to accounts closed down by the consumer.

It seems that Congress in ARRA agreed with CDT, for Congress did not extend HIPAA directly to PHRs. But to the extent that PHRs enter into agreements with covered entities to allow those entities to offer a PHR to their patients, they may be covered as business associates (which would make them directly accountable for complying with key HIPAA provisions).¹⁵ CDT has argued for a narrow interpretation of this provision.¹⁶

Instead of extending HIPAA to all PHRs, Congress directed HHS to work with the FTC to come up with recommendations for privacy and security protections for PHRs. This PHR “study” must also include a recommendation for which agency (HHS, FTC or both) should have responsibility for regulating these entities – as well as a “timeline” for regulation, although Congress stopped short of calling for specific regulations.

For PHRs offered by entities that are not part of the traditional health care system, it is critical that regulators understand the business model behind these products, which will largely rely on advertising revenue and partnerships with third-party applications – likely suppliers of health-related products and services. It will not be adequate, in our view, to depend heavily on consumer authorization. Consistent with CDT’s views about the role of consumer consent in protecting health information, relying too heavily on consumer authorization for use of information shifts the burden of protecting privacy solely to the consumer and puts the bulk of the bargaining power on the side of the entity offering the PHR.¹⁷ For consumers to truly trust PHRs – and for these tools to flourish as effective mechanisms for engaging more consumers in their health care – clear rules are needed regarding marketing and commercial uses that will better protect consumers. CDT has testified before the National Committee on Vital and Health Statistics (NCVHS) on protections for PHRs, and is finalizing a comprehensive paper to be released this spring. See Appendix A for a copy of CDT’s comments to NCVHS.

Ensuring Comprehensive Coverage – Downstream Uses of Data

As noted above, HIPAA applies only to “covered entities.” However, under the HIPAA Privacy Rule, entities that contract with HIPAA covered entities to perform particular services or functions on their behalf using protected, identifiable health information (or PHI) are required to enter into “business associate” agreements.¹⁸ Such agreements may not authorize the business associate to access, use or disclose information for activities that the covered entity itself could not do under HIPAA.¹⁹ The agreements also are required to establish both the permitted and required uses and disclosures of health information by the business associate,²⁰ and to specify that the business associate “will not use or further disclose the information other than as permitted or required by the contract or as required by law.”²¹ Business associates are also required to, at the termination of a business associate agreement and “if feasible,” return or destroy personal data they receive from a covered entity. If return or destruction is not feasible, the contract must limit any further uses and disclosures to those that make the return or destruction of the information infeasible.²²

¹⁵ ARRA, Section 13408.

¹⁶ See <http://e-caremanagement.com/privacy-law-showdown-legal-and-policy-analysis/>.

¹⁷ See Rethinking the Role of Consent in Protecting Health Information Privacy (January 2009) <http://www.cdt.org/healthprivacy/20090126Consent.pdf>.

¹⁸ 45 CFR 164.502(e)(1) & (2).

¹⁹ 45 CFR 164.504(e)(2)(i).

²⁰ *Id.*

²¹ 45 CFR 164.504(e)(2)(ii)(A)

²² 45 CFR 164.504(e)(2)(I).

This combination of provisions place clear limits on what a business associate can do with health information received from a covered entity. However, one large business associate has been accused of using data they receive from covered entities to support other business objectives,²³ and some privacy advocates have long suspected that such practices are more widespread.

If such practices by business associates are in violation of the terms of their contracts with covered entities, ARRA strengthened the ability of government authorities to hold business associates accountable for such violations. Historically enforcement of a business associate agreement was largely in the discretion of the covered entity, and authorities could hold covered entities liable for the actions of their contractors only in limited circumstances. However, under ARRA, federal and state authorities can hold business associates directly accountable for failure to comply with their contracts.²⁴ Resolving these concerns may primarily be an issue of stronger enforcement of the law. But it's also possible that the contracts expressly or implicitly authorize more expansive uses and disclosures of data (presumably based on interpretations of the Privacy Rule). CDT will be exploring this in more detail in 2010, because, as explained in more detail below, organizations that facilitate the exchange of personal health information are now covered under HIPAA as business associates. It will be critical to ensure that an exchange's use, access and disclosure of data is both lawful and also consistent with building public trust in health IT.

The Uncertainty of Exchange Networks

In an effort to promote the more widespread exchange of electronic health information among health care providers, electronic information exchange networks are cropping up across the country to facilitate exchange among providers in local communities, or in states or geographic regions. ARRA includes significant funding to states to facilitate health information exchange, and the HHS Office of the National Coordinator for Health IT is targeting additional funding to 15 communities who have established basic electronic health information exchange infrastructures to enable them to more rapidly progressed to more advanced levels of data exchange to improve treatment and overall health outcomes.²⁵

Exchange networks will play an essential role in achieving the data liquidity that is essential to meaningful health reform. However, there are numerous policy issues that will need to be resolved to ensure the promise of these networks can be realized. Critical questions include who can access data from these networks and for what purposes; what level of security should be required; how can networks be leveraged to enhance patient access to data; and how will policies and standards applicable to networks be enforced. Until the passage of ARRA, it was uncertain whether these exchanges would be covered by HIPAA. ARRA made it clear that at least some models of exchange are to be treated as business associates under HIPAA.²⁶ As a result, those entities are now required to directly comply with key HIPAA regulatory provisions.

But the application of the HIPAA business associate rules to these networks does not resolve many of the critical policy questions that must be addressed. So long as the business model and future direction of most networks remain uncertain, consumers and patients should ideally have an least have an option to opt-out of having their health information accessible through these networks.

²³ See <http://www.alarmedaboutcvscaremark.org/fileadmin/files/pdf/an-alarming-merger.pdf>, pages 14-16.

²⁴ ARRA, section 13404.

²⁵ <http://healthit.hhs.gov/blog/onc/index.php/2009/12/02/beacon-communities-a-proving-ground-for-health-it/>

²⁶ ARRA, Section 13408.

The HIPAA De-Identification Standard

HIPAA's protections do not extend to health information that qualifies as "de-identified" under the Privacy Rule. Thus, covered entities may provide de-identified data to third parties for uses such as research and business intelligence without regard to HIPAA requirements regarding access, use and disclosure. In turn, these entities may use this data as they wish, subject only to the terms of any applicable contractual provisions (or state laws that might apply). If a third party then re-identifies this data – for example, by using information in its possession or available in a public database – the re-identified personal health information would not be subject to HIPAA.²⁷ It could be used for any purpose unless the entity holding the re-identified data was a covered entity (or had voluntarily committed to restrictions on use of the data).

There is value to making data that has a very low risk of re-identification available for a broad range of purposes, as long as the standards for de-identification are rigorous, and there are sufficient prohibitions against re-identification. This is not the case today. A number of researchers have documented how easy it is to re-identify some data that qualifies as de-identified under HIPAA.²⁸ CDT has urged HHS to revisit the current de-identification standard in the Privacy Rule (in particular, the so-called "safe harbor" that deems data to be de-identified if it is stripped of particular data points) to ensure that it continues to present de minimis risk of re-identification. At the same time, policymakers should enact provisions to ensure data recipients can be held accountable for re-identifying data.²⁹

Minimum Necessary and Encouraging Use of "Lesser Identified" Data

Although the HIPAA provisions for de-identified data need improvement, CDT also recognizes that privacy risks are lessened when data has been anonymized to the greatest extent possible, as long as there are enforceable prohibitions against re-identification. In particular, many non-treatment uses of health data -- including quality, research and public health -- can be done with data where sufficient patient identifiers have been removed to make it anonymous to the recipient. Unfortunately, federal and state privacy laws do not sufficiently promote the use of "lesser identified" data. Instead, they permit (in the case of HIPAA) or require (in the case of many state reporting laws) the use of fully identifiable data (including patient names, addresses, phone numbers, etc.), providing little incentive to remove identifiers from data before its use.

Under the collection and use limitations of fair information practices, data holders and recipients must collect, use and disclose only the minimum amount of information necessary to fulfill the intended purpose of obtaining or disclosing the data. The Privacy Rule incorporates these principles in the "minimum necessary" standard, which requires covered entities to use only the minimum necessary amount of data for most uses and disclosures other than treatment. This standard is intended to be flexible, but the Department of Health and Human Services (HHS) has not issued any meaningful

²⁷ If a covered entity has a reasonable basis for knowing that the recipient of "de-identified" data will be able to re-identify it, the data does not qualify as de-identified. See 45 C.F.R. 164.514(b)(2)(ii).

²⁸ See, for example, Salvador Ocha, Jamie Rasmussen, Christine Robson, and Michael Salib, *Reidentification of Individuals in Chicago's Homicide Database, A Technical and Legal Study* (November 2008),

<http://web.mit.edu/sem083/www/assignments/reidentification.html> (accessed November 20, 2008).

²⁹ See http://www.cdt.org/healthprivacy/20090625_deidentify.pdf for a more comprehensive discussion of CDT's views on the HIPAA de-identification standard.

guidance on this standard. As a result, covered entities and their business associates frequently express concerns about how to implement it.

The Privacy Rule does provide for two anonymized data options – de-identification (as discussed above) and the limited data set, which can be used for research, public health and health care operations (as long as the covered entity enters into a data use agreement with the data recipient). These anonymized data sets provide greater privacy protection for individuals, but a significant amount of identifying information must be removed before data qualifies as a limited data set or de-identified under HIPAA. Thus, a number of health industry stakeholders have raised concerns that these data sets have limited utility for a range of important health care purposes.

ARRA attempts to strengthen the Privacy Rule’s collection and use limitation by strongly encouraging covered entities to use a limited data set to comply with the minimum necessary standard, as long as limited data is sufficient to serve the purposes for the data access or disclosure.³⁰ This section of ARRA also requires the HHS Secretary to issue guidance on how to comply with the minimum necessary standard; when such guidance goes into effect, the directive to use the limited data set expires. CDT will be advocating for HHS to issue guidance on the minimum necessary standard that provides greater options for the use of “lesser identified” data for a number of routine purposes for which fully identifiable data can now be used, with sufficient accountability for re-identification.

Marketing

The use of sensitive medical information for marketing purposes is one of the most controversial practices affecting health privacy. The HIPAA Privacy Rule has provisions intended to limit the use of health data in marketing, but it historically was subject to a number of exceptions. There also has been little regulatory or legislative investigation of health marketing practices.

In ARRA, Congress took some steps to tighten the definition of “marketing” in the Privacy Rule. Under the new provisions, communications that are paid for by third parties are marketing – even if those communications would otherwise not be construed as marketing because they relate to an individual’s health or suggest treatment alternatives. But even this new provision includes exceptions that could swallow the rule. For example, entities do not need a patient’s authorization to send remunerated communications about a drug or biologic that the patient is currently taking.

In addition, ARRA specifies that entities may receive outside payment for “treatment” – which suggests that communications sent for treatment purposes that are paid for by third parties can be sent without requiring patient authorization. CDT recognizes that broad prohibitions restricting the right to use health information to communicate with patients for treatment purposes are counterproductive. But because treatment is broadly defined in the HIPAA Privacy Rule, this exception may result in some purely marketing communications being made with patients’ health information without their prior authorization.

Securing the right set of provisions to protect patients from abuse of their personal health information for marketing purposes has been difficult to achieve at the federal level. One way to close this gap in the Privacy Rule is to restrict who may access data for treatment or care management purposes to professional caregivers directly involved in the individual’s treatment. Such a measure could greatly restrict access to and abuse of protected health information from provider or health plan electronic medical records (or health information exchanges) for what are largely marketing uses.

³⁰ ARRA, Section 13405.

Enforcement

When Congress enacted HIPAA in 1996, it included civil and criminal penalties for noncompliance, but those rules have never been adequately enforced.³¹ The Office for Civil Rights (OCR) within HHS, charged with enforcing the HIPAA privacy regulations, had not levied a single penalty against a HIPAA-covered entity in the nearly five years since the rules were implemented, even though that office found numerous violations of the rules.³² The Justice Department had levied some penalties under the criminal provisions of the statute, but a 2005 opinion from DOJ's Office of Legal Counsel (OLC) expressly limited the application of the criminal provisions to covered entities, forcing prosecutors to turn to other laws in order to criminally prosecute certain employees of covered entities who have criminally accessed, used or disclosed a patient's protected health information.³³

A lax enforcement environment sends a message to entities that access, use and disclose protected health information that they need not devote significant resources to compliance with the rules. Without strong enforcement, even the strongest privacy and security protections are but an empty promise for consumers. Further, HIPAA has never included a private right of action, leaving individuals dependent on government authorities to vindicate their rights.

In ARRA, Congress took a number of steps to strengthen HIPAA enforcement.³⁴ State attorneys general are now expressly authorized to bring civil enforcement actions under HIPAA. Although state authorities are limited in the civil monetary penalties they can pursue (such fines can only be imposed at the previous statutory level - \$100 per violation, with a \$25,000 maximum for repeat violations), the additional enforcement resources under HIPAA should help ensure that the law is more vigorously enforced.

Other important improvements to HIPAA enforcement include the following:

- As mentioned above, business associates are now directly responsible for complying with key HIPAA privacy and security provisions and can be held directly accountable for any failure to comply.
- Civil penalties for HIPAA violations have been significantly increased. Under ARRA, fines of up to \$50,000 per violation (with a maximum of \$1.5 million annually for repeated violations of the same requirement) can now be imposed.³⁵
- HHS is required to impose civil monetary penalties in circumstances where the HIPAA violation constitutes willful neglect of the law.
- The U.S. Department of Justice can now prosecute individuals for violations of HIPAA's criminal provisions.
- The HHS Secretary is required to conduct periodic audits for compliance with the

³¹ Richard Alonso-Zaldivar, "Effectiveness of medical privacy law is questioned," Los Angeles Times, 9 April 2008.

³² "Effectiveness of medical privacy law is questioned," Richard Alonso-Zaldivar, Los Angeles Times (April 9, 2008) http://www.latimes.com/business/la-na-privacy9apr09_0_5722394.story.

³³ See <http://www.americanprogress.org/issues/2005/06/b743281.html> for more information on the OLC memo and the consequences.

³⁴ See Sections 13409-13411 of ARRA.

³⁵ Of note, the increased penalties went into effect on the day of enactment – February 17, 2009.

HIPAA Privacy and Security Rules. (The HIPAA regulations provide the Secretary with audit authority, but this authority was rarely if ever used during the Bush Administration.)

The ARRA provisions are a major advancement in enforcement of federal health privacy laws, but individuals are still dependent on federal or state authorities to enforce the law, as there is no private right of action. ARRA does require the HHS Secretary to establish a methodology to allow individuals harmed by HIPAA violations to receive a percentage of any civil penalties or civil monetary settlements obtained by the government – but this falls short of giving individuals the tools to directly enforce their rights. CDT believes that a private right of action should be part of any enforcement scheme. We recognize that providing a private right of action to pursue every HIPAA complaint – no matter how trivial – would be inappropriate and disruptive, but Congress should give consumers some right to privately pursue recourse in certain circumstances. For example, policymakers could create compliance safe harbors that would relieve covered entities and their business associates of liability for violations if they meet the privacy and security standards but would allow individuals to sue if they could prove the standards had not been met. Another suggestion is to limit the private right of action to only the most egregious HIPAA offenses, such as those involving intentional violations or willful neglect.

Minors

The FTC has specifically asked for input on whether minor’s information should be subject to more stringent privacy standards. As the FTC may be aware, a number of states permit “mature” minors to obtain certain types of health care without parental or guardian consent.³⁶ The HIPAA Privacy Rule essentially defers to state law with respect to access to minor’s health information by a parent, or whether the minor has the right to control access to his or her information.³⁷ Restrictions on the extent to which minors can seek and share health information on-line (or parental consent requirements) could significantly undermine the intent of mature minor laws, which is to ensure that minors are not deterred from seeking appropriate medical care.

Placing stricter controls on information that can be sent to minors also implicates free speech. The First Amendment protects *both* the right of minors to receive the information and the right of speakers to reach an audience of minors. We urge FTC to review the final report of the Internet Safety Technical Task Force on Enhancing Child Safety & Online Technologies, which we are also submitting as comments for this Roundtable.³⁸

Conclusion

Thank you for the opportunity to present these remarks in support of strengthening privacy and security protections for personal health information.

Deven McGraw
Director, Health Privacy Project
deven@cdt.org
202-637-9800 x119

³⁶ See <http://www.guttmacher.org/pubs/tgr/03/4/gr030404.pdf> for a general discussion of these laws.

³⁷ 45 CFR 164.502(g)(3)(ii) and Office for Civil Rights, HHS, Guidance on Personal Representatives (April 3, 2003) available at <http://www.hhs.gov/ocr/hipaa/guidelines/personalrepresentatives.pdf>.

³⁸ <http://cyber.law.harvard.edu/pubrelease/istff/>

Statement of Deven McGraw
Director, Health Privacy Project
Center for Democracy & Technology

Before the
National Committee on Vital and Health Statistics
Subcommittee on Privacy, Confidentiality & Security

Hearing on Personal Health Records

June 9, 2009

Thank you for holding this hearing on personal health records and for the opportunity to testify. CDT is a non-profit public interest organization founded in 1994 to promote democratic values and individual liberties for the digital age. CDT works to keep the Internet open, innovative and free by developing practical, real-world solutions that enhance free expression, privacy, universal access and democratic participation. The Health Privacy Project, which has more than a decade of experience in advocating for the privacy and security of health information, was merged into CDT last year to take advantage of CDT's long history of expertise on Internet and information privacy issues. Our mission is to develop policies and practices that will better protect the privacy and security of health information on-line and build consumer trust in e-health systems.

Surveys consistently demonstrate the support of the American public for health IT. At the same time, however, the public is very concerned about the risks health IT poses to health privacy. A system that makes greater volumes of information available more efficiently to improve care will be an attractive target for those who seek personal health information for commercial gain or inappropriate purposes. Building public trust in health IT systems is critical to realizing the technology's potential benefits. While some persist in positioning privacy as an obstacle to achieving the advances that greater use of health IT can bring, it is clear that the opposite is true: enhanced privacy and security built into health IT systems will bolster consumer trust and confidence and spur more rapid adoption of health IT and realization of its potential benefits.

This is particular true in the case of personal health records. Personal health records (PHRs) hold significant potential for consumers and patients to become key, informed decision-makers in their own health care. PHRs can be drivers of needed change in our health care system by providing individuals with options

for storing and sharing copies of their health records, as well as options for recording, storing, and sharing other information that is relevant to health care but is often absent from official medical records (such as pain thresholds in performing various activities of daily living, details on side effects of medication, and daily nutrition and exercise logs). However, in order to feel comfortable using PHRs, consumers need assurance that their information will be protected by reasonable privacy and security safeguards.

It is often difficult or impossible to establish effective privacy protections retroactively, and restoring public trust that has been significantly undermined is much more difficult—and more expensive—than building it at the start. Now, in the early stages of adoption of PHRs, is the critical window for addressing privacy.

Our testimony below discusses the need for a comprehensive privacy and security framework to protect consumers using personal health records and pave the way for the more widespread adoption of these potentially transformative tools; a model for such a framework; the need for (and lack of) consistent policies governing PHRs; and why the HIPAA Privacy Rule – in its current form – is not appropriate vehicle for protecting the privacy of consumers using PHRs.

▣ Why Privacy and Security Protections are Critical

Recent survey data from the Markle Foundation shows that consumers see the enormous potential of PHRs – but that privacy and security concerns are a major factor impeding their adoption. According to this survey, released in June 2008, four in five U.S. adults believe that electronic personal health records (PHRs) would help people:

- Check for errors in their medical records (87 percent).
- Track health-related expenses (87 percent).
- Avoid duplicated tests and procedures (86 percent).
- Keep their doctors informed of their health status (86 percent).
- Move more easily from doctor to doctor (86 percent).
- Manage the health of loved ones (82 percent).
- Get treatments tailored to health needs. (81 percent).
- Manage their own health and lifestyle (79 percent).¹

Only a small percentage of survey respondents – 2.7% – reported having a PHR, although among this group, four in five described their PHR as “valuable.”² Of

¹ http://www.connectingforhealth.org/news/pressrelease_062508.html.

those who said they were not interested in having a PHR, more than half (57%) cited privacy concerns as a reason. Specifically, 24% reported their privacy concerns as high; 49-56% characterized them as moderate; and only 20-27% reported their privacy concerns as low.³ According to Alan Westin, who designed the survey, “[t]his pattern of health privacy intensity suggests that [73-80%] of the public will want to be assured of robust privacy and security practices by online PHR services, if they are to join those offerings.”⁴ It is clear that privacy and security protections are needed to spark greater interest in and use of PHRs.

▣ We Need a Comprehensive Privacy and Security Framework That Will Build Public Trust in PHRs

To build public trust in PHRs and similar consumer-based health tools, we need a comprehensive privacy and security framework that targets the risks to consumers using them and is flexible enough to allow for innovation to meet a wide array of consumer needs. Policymakers need not start from scratch in developing this framework. In June 2008, Markle Connecting for Health released the Common Framework for Networked Health Information,⁵ outlining consensus privacy and security policies for PHRs and other “consumer access” services. This framework — which was developed and supported by a diverse and broad group including technology companies, consumer organizations like CDT, and HIPAA-covered entities⁶ — was designed to meet the dual challenges of making personal health information more readily available to consumers, while also protecting it from unfair or harmful practices. It includes four overviews and 14 specific technology and policy approaches for consumers to access health services, to obtain and control copies of health information about them, to authorize the sharing of that information with others, and sound privacy and security practices.⁷

The American Recovery and Reinvestment Act of 2009 (ARRA or the economic stimulus legislation) requires HHS (in consultation with the FTC) to report to Congress no later than February 18, 2010, with recommendations for privacy and security requirements for PHR vendors and related entities that are not covered by HIPAA as either covered entities or business associates.⁸ In recent public comments, we urged HHS to rely on the Markle Connecting for Health

² Id.

³ Id.

⁴ Id.

⁵ See www.connectingforhealth.org/phti.

⁶ See list of endorsers of the Markle Connecting for Health Common Framework for Networked Personal Health Information at the following URL: <http://www.connectingforhealth.org/resources/CCEndorser.pdf>.

⁷ For a short summary of the overview and principles, please see <http://www.connectingforhealth.org/resources/CCPolicyBrief.pdf>.

⁸ Section 13424(b) of ARRA.

framework in developing its recommendations.⁹ CDT also recently held an all-day workshop on PHRs, bringing together major vendors, patients, consumer organizations, other health care stakeholders and “health 2.0” innovators to begin addressing the question of which elements of the framework should be incorporated into regulations and which should be enforced through other mechanisms like chain-of-trust agreements and business best practices. We will issue a paper with more specific recommendations for regulating PHRs this summer.

▣ PHRs should be Governed by Consistent Policies; Current Federal Policies are Insufficient or Inadequate

Among the policies endorsed in the Markle framework is that individuals should have the choice of whether or not to open a PHR account, and they should choose what entities may access or exchange information into or out of that account.¹⁰ This foundational policy is reflected in the definition of a PHR in the economic stimulus legislation: “an electronic record of information on an individual *“that is managed, shared, and controlled by or primarily for the individual.”*”¹¹

At the core of the framework is the belief that PHRs should be governed by a consistent and meaningful set of privacy and security policies, regardless of the type of entity offering them. It will be confusing and potentially harmful to consumers to have different protections and rules for PHRs depending on the legal status or business model of the offering entity, and even more so if the policies do not consistently support meaningful consumer participation in and control of these emerging and powerful tools.

There is no such consistent regulatory framework in place today. PHRs are regulated by HIPAA only if they are offered by covered entities or business associates acting on their behalf. If they are not regulated by HIPAA, as is the case for most PHRs offered by Internet companies and employers,¹² consumer privacy may be protected only by the PHR provider’s privacy and security policies (and potentially under certain state laws that apply to uses and disclosures of certain types of health information), and if these policies are violated, the Federal Trade Commission (FTC) may bring an action against a company for failure to abide by its privacy policies. The policies of PHR vendors range from very good to seriously deficient.¹³ In some cases, other federal laws

⁹ http://www.cdt.org/healthprivacy/20090521_RFI_comments.pdf

¹⁰ See <http://www.connectingforhealth.org/phti/reports/cp3.html>.

¹¹ Section 13400 of ARRA.

¹² We note that HIPAA requires these entities to enter into business associate agreements with covered entities under some circumstances. See Section 13408 of ARRA.

¹³ The HHS Office of the National Coordinator commissioned a study in early 2007 of the policies of over 30 PHR vendors and found that none covered all of the typical criteria found in privacy policy. For example, only two policies described what would happen to the data if the vendor were sold or went out of business, and only one had a policy with respect to accounts closed down by the consumer.

that govern storage and transmission of electronic communications or that regulate Internet sites may apply, but none provide comprehensive privacy and security protections for health information, and none were enacted specifically to protect consumers using PHRs.

The economic stimulus legislation provides opportunities to advance a consistent approach to regulating PHRs regardless of the source, but further action from the Administration is needed to make this a reality. The study to be conducted by HHS and FTC with respect to privacy and security for PHRs is only required to consider those not already covered by HIPAA. HHS should extend this study to look at creating a consistent set of regulations for PHRs across the board.

Consistent with this view, CDT and the Markle Foundation jointly urged HHS, in implementing the new breach notification rules applicable to PHRs, to define a breach as the “acquisition, use or disclosure” of information in a PHR without the authorization of the individual.¹⁴ We posited that this approach is required to appropriately implement the PHR definition in the stimulus legislation as being an electronic record of information on an individual “that is managed, shared, and controlled by or primarily for the individual.”¹⁵ It is also consistent with the FTC’s proposed breach notification standard, which requires notification when information in a PHR is acquired without individual authorization.¹⁶ We urge this Subcommittee and NCVHS to develop recommendations that support a consistent policy environment for consumers using PHRs.

▣ Application of the HIPAA Privacy Rule – in Its Current Form - is Not the Answer

Although some PHRs are currently covered by HIPAA, the need for consistent policies does not make it appropriate to automatically extend HIPAA coverage in its current form to all PHRs. The HIPAA rules were based on fair information practices, and with respect to the sharing of health information among physicians, hospitals and health plans, HIPAA represents the foundation upon which a comprehensive framework of protections for e-health should be built. But HIPAA was specifically designed to regulate only the sharing of information among traditional health care system entities. As a result:

- personal health information is permitted to flow without patient authorization for treatment, payment, and health care operations;

¹⁴ http://www.cdt.org/healthprivacy/20090521_RFI_coments.pdf. We noted in our comments that our suggestions with respect to regulation of PHRs should not be interpreted to suggest any changes in the rules governing a covered entity’s operational record (e.g., their legal medical record) and its permitted uses of data captured in such operational records of the covered entity.

¹⁵ Id. (emphasis added).

¹⁶ Section 13407(f)(1) of ARRA.

- other uses are permitted without consent pursuant to certain procedures and safeguards (i.e., disclosure to researchers, law enforcement); and
- a number of uses—such as to employers or for marketing and any uses not expressly mentioned in the Privacy Rule— require express, uncoerced patient authorization, but the marketing provisions in particular have historically provided weak privacy protections.

These aspects of the Privacy Rule (among others) render it ineffective at protecting PHRs. As a result, application of the Privacy Rule in its current scope may do more harm than good.¹⁷ In particular, the Privacy Rule’s reliance on individual authorization for marketing and commercial uses places people in an unfair and potentially dangerous situation, shifting the burden of protecting privacy solely to the individual and putting the bulk of the bargaining power on the side of the entity offering the PHR. A few of the most troubling problems are:

- Research on consent on the Internet shows that most people do not read the details of consent forms before signing them, and those that do often do not understand the terms. Many wrongly assume that the existence of a privacy policy means that their personal information will not be shared, even when the policy and the accompanying consent form say just the opposite. And for free web-based products like PHRs, consent to the statement of uses and disclosures (a.k.a. the “privacy policy”) will likely be required in order to use the service.¹⁸
- A major business model to support third-party PHRs is advertising revenue and partnerships with third-party suppliers of health-related products and services. As a result, people using these tools will be more likely to be marketed to on the basis of health information in their PHI. They will likely be subjected to the tools that Internet companies typically use to gather information about consumer preferences (such as cookies), so that the companies can target them with specific ads or product offers. Their data may be more likely to be sold to third parties (such as pharmaceutical companies and health insurers). They also will likely be solicited by the PHR’s formal and informal business partners (for example, diabetes management programs sponsored by the diabetes meter companies, weight loss and fitness programs, etc.), who also will likely solicit individuals to share their data and may use that data for multiple business purposes (including selling it).

For PHRs to flourish, we believe clear rules are needed regarding marketing and commercial uses of information that will better protect consumers by restricting PHR vendors from engaging in certain practices, or by providing individuals

¹⁷ Because of our concerns about relying on the HIPAA Privacy Rule to protect consumers using PHRs, we recently blogged about the need to narrowly interpret the provision in ARRA requiring vendors of PHRs to enter into business associate agreements and therefore be covered by HIPAA. See <http://e-caremanagement.com/privacy-law-showdown-legal-and-policy-analysis/>.

¹⁸ For additional details on CDT’s view of the role of individual consent in protecting health information, please see <http://www.cdt.org/healthprivacy/20090126Consent.pdf>.

with certain rights—in other words, a much stronger and more comprehensive package of privacy and security safeguards than merely affording people the right to check a box acknowledging the uses and disclosures of their information. This may mean the application of certain provisions in HIPAA (for example, HHS should consider whether the HIPAA Security Rule provides adequate security protections for PHRs), but for the most part will require a different set of requirements.

If the Privacy Rule is nevertheless viewed as the appropriate vehicle for strengthening or expanding privacy protections for consumers who use PHRs, CDT believes the HHS Secretary should promulgate HIPAA rules specific to PHRs that respond to the unique issues they raise. (For just one example, the rules permitting covered entities to use personal health information without express authorization for treatment, purposes, and health care operations should not be applied to PHRs.) CDT further recommends that Secretary consult with the FTC, which has experience in issues related to online privacy and consumer protection, in developing these rules.

▣ Establishing Privacy Protections for PHRs

The economic stimulus legislation – which tasks HHS and FTC with jointly coming up with recommendations for privacy and security requirements for PHRs – is the right approach for ultimately establishing comprehensive privacy and security protections for consumers using these new health tools. As noted above, we hope HHS will consider establishing consistent rules regarding PHRs that are based on the Markle framework regardless of the type or legal status of the entities offering them. For PHRs offered by entities that are not part of the traditional health care system, it is critical that regulators understand the business model behind these products, which will largely rely on advertising revenue and partnerships with third-party suppliers of health-related products and services. Even for PHRs offered by HIPAA covered entities, consumer trust in these products will be built through a consistent set of rules regarding access to and disclosure of information.

As noted above, patients should have the right to control information in their PHRs, but relying solely or disproportionately on consumer authorization for use of information shifts the burden of protecting privacy solely to the consumer and puts the bulk of the bargaining power on the side of the entity offering the PHR. For consumers to truly trust PHRs – and for these tools to flourish as effective mechanisms for engaging more consumers in their health care – such consumer consent should be situated within a clear framework of rules regarding marketing and commercial uses that will better protect consumers.

For example, in order to ensure that consumers do not inadvertently grant blanket authorization for use of their data, regulators may have to address the form and content of the terms of service and the privacy policies for systems offering PHR services. The foundation of PHRs should be opt-in (i.e., affirmative as opposed to implied consent), but even opt-in consent can be too general.

Therefore, baseline regulatory standards might specify particular uses or disclosures for which independent consent must be obtained. For example, it might be required that consent to disclose data for marketing or commercial purposes must be obtained independently of other consent. Special consent might also be required for research uses of data, even if the data is de-identified or aggregated.

Policymakers may find it necessary to go further and prohibit certain uses or disclosures of data in PHRs, regardless of consent. Compelled disclosures pose a particular problem in the contexts of employment, credit or insurance, where individuals are often compelled to sign authorizations granting employers, banks, insurers, and others access to their health records for non-medical purposes. While the problem of these disclosures, which are nominally voluntary but in fact compelled, applies to traditional health records, it is exacerbated with PHRs, which may contain not only copies of provider records but also user-generated data not revealed even to a doctor. If PHRs are to be encouraged, the best course may be to prohibit their use in the context of employment, credit or insurance. Congress has already moved in this direction with the Genetic Information Nondiscrimination Act of 2008 (GINA), which prohibits employers from using genetic information to make employment decisions and prohibits health insurers from using such information to make coverage and underwriting determinations. Under GINA, individuals cannot be asked for permission to use their genetic information for these purposes.¹⁹

A comprehensive privacy framework would also include limits on downstream recipients of data from PHRs. As noted above, the revenue model to support many Internet-based PHRs will be partnerships with third parties who will offer services or “applications” to PHR account holders, which means a consumer’s PHR data may pass to many organizations. Contractual agreements will be necessary to bind business partners to particular privacy and security policies, such as a commitment not to re-disclose the data or to use it for purposes other than those for which consent was granted. However, such contractual commitments will be insufficient to build consumer trust in PHRs. Even if such contracts were required to contain certain elements, consumers could not be assured of consistent enforcement.

▣ Conclusion

To establish greater public trust in PHRs and pave the way for their adoption, we need a comprehensive and consistent privacy and security framework that is vigorously enforced. The Markle Common Framework for Networked Personal Health Information, developed through a multi-stakeholder process and endorsed by a broad group of stakeholders, provides a consistent policy framework for PHRs. HHS and FTC should consider which elements of the

¹⁹ The Johns Hopkins University, Genetics and Public Policy Center, Summaries of GINA Title I (Health Insurance) and GINA Title II (Employment), <http://www.dnapolicy.org/resources/GINATitleIsummary.pdf> and <http://www.dnapolicy.org/resources/GINATitleIIsummary.pdf> (accessed November 20, 2008).

framework should be imposed by regulation and which should be adopted through other mechanisms. From traditional health entities to new PHR developers to policymakers, all have an important role to play in protecting consumers using PHRs.

Enhancing Child Safety & Online Technologies:

FINAL REPORT OF THE
INTERNET SAFETY TECHNICAL TASK FORCE

To the Multi-State Working Group on Social Networking
of State Attorneys General of the United States

DECEMBER 31, 2008



Berkman

The Berkman Center for Internet & Society
at Harvard University

ENHANCING CHILD SAFETY AND ONLINE TECHNOLOGIES:
FINAL REPORT OF THE INTERNET SAFETY TECHNICAL TASK FORCE
TO THE MULTI-STATE WORKING GROUP ON SOCIAL NETWORKING
OF STATE ATTORNEYS GENERAL OF THE UNITED STATES

December 31, 2008

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

Chair: Professor John Palfrey

Co-Director: Dena T. Sacco

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

Chair, Technology Advisory Board: Laura DeBonis

Coordinator: Jessica Tatlock

Task Force Members:

AOL/Bebo

Aristotle

AT&T

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

Center for Democracy & Technology

Comcast

Community Connect Inc.

ConnectSafely.org

Enough Is Enough

Facebook

Family Online Safety Institute

Google Inc.

IAC

ikeepsafe

IDology, Inc.

Institute for Policy Innovation

Linden Lab

Loopt

Microsoft Corp

MTV Networks/Viacom.

MySpace and Fox Interactive Media

National Center for Missing & Exploited Children

The Progress & Freedom Foundation

Sentinel Tech Holding Corp.

Symantec

Verizon Communications, Inc.

Xanga

Yahoo!, Inc.

Wiredsafety.org

December 31, 2008

To the Multi-State Working Group on Social Networking of State Attorneys General of the United States:

On behalf of the Internet Safety Technical Task Force, I am pleased to transmit to the 52 Attorneys General on the Multi-State Working Group the Task Force's Final Report on the role and the promise of technologies to reduce the risk to minors of harmful contact and content on the Internet. Along with the quarterly reports submitted throughout the year to the Attorneys General and the evaluation criteria included in the Technology Advisory Board's submission, this Report fulfills the Task Force's remit to report the results of its study no later than December 31, 2008.

I would like to thank in particular Attorneys General Richard Blumenthal of Connecticut and Roy Cooper of North Carolina, and their respective staffs, for their support throughout this process and for their leadership – over many years – to help protect children from the risk of harm online. I was especially pleased to have been hosted by Attorney General Martha Coakley, who has been a key figure, along with her staff, in protecting children online in the Commonwealth of Massachusetts and nationally. The leadership of these Attorneys General and their colleagues, on this and many related issues – including identity theft, spam, phishing, and cybersecurity – is an important driver in making the Internet a safer place for all of us.

I would also like to take this opportunity to recognize the outstanding efforts of all of the Task Force members and their respective organizations. I am grateful, too, to the Technology Advisory Board and the Research Advisory Board for their contributions to this process. This Task Force was a collaborative effort, convened over a very short period of time, on an issue of the utmost importance to our society. We all look forward to working on the next steps to help implement the recommendations included in this report.

Sincerely,

John Palfrey
Chair, Internet Safety Technical Task Force
Harvard Law School
1545 Massachusetts Avenue
Cambridge, MA 02138

TABLE OF CONTENTS

Executive Summary

I. Introduction

II. Methodology

III. Summary Report from the Research Advisory Board

IV. Summary Report from the Technology Advisory Board

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

VI. Analysis

VII. Recommendations

VIII. Conclusion

Appendix A: Joint Statement on Key Principles of Social Networking Safety

Appendix B: Task Force Project Plan

Appendix C: Literature Review from the Research Advisory Board

Appendix D: Report of the Technology Advisory Board and Exhibits

Appendix E: Submissions from Social Network Sites

Appendix F: Statements from Members of the Task Force

Executive Summary

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

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

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

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

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

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

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

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

The Task Force remains optimistic about the development of technologies to enhance protections for minors online and to support institutions and individuals involved in protecting minors, but cautions against overreliance on technology in isolation or on a single technological approach. Technology can play a helpful role, but there is no one technological solution or specific combination of technological solutions to the problem of online safety for minors. Instead, a combination of technologies, in concert with parental oversight, education, social services, law enforcement, and sound policies by social network sites and service providers may assist in addressing specific problems that minors face online. All stakeholders must continue to work in a cooperative and collaborative manner, sharing information and ideas to achieve the common goal of making the Internet as safe as possible for minors.

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

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

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, 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. 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. 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 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.

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). An early study 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). 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.

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 uses one of the technologies submitted to the Task Force to identify and remove registered sex offenders from its site. 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. 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.

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.

APPENDIX A:

Joint Statement on Key Principles of Social Networking Safety



Roy Cooper North Carolina Attorney General

For Immediate Release
Date: January 14, 2008

Contact: Noelle Talley
Phone: 919/716-6413

AG Cooper announces landmark agreement to protect kids online

Cooper led effort to forge national agreement with MySpace to make social networks safer

New York: In a victory for social networking safety, Attorney General Roy Cooper and 49 other attorneys general today announced that MySpace has agreed to significant steps to better protect children on its web site, including creating a task force to explore and develop age and identity verification technology.

“We’re joining forces to find the most effective ways to keep young children off these sites and to protect the kids who do use them,” said Cooper. “This agreement sets a new standard for social networking sites that have been quick to grow but slow to recognize their responsibility to keep kids safe.”

MySpace acknowledged in the agreement the important role of age and identity verification technology in social networking safety and agreed to find and develop on-line identity authentication tools. Cooper and the other attorneys general advocate age and identity verification, calling it vital to better protecting children using social networking sites from online sexual predators and inappropriate material.

Other specific changes and policies that MySpace agreed to develop include: allowing parents to submit their children’s email addresses so MySpace can prevent anyone using those email addresses from setting up profiles, making the default setting “private” for profiles of 16- and 17-year-olds, promising to respond within 72 hours to inappropriate content complaints and committing more staff and/or resources to review and classify photographs and discussion groups.

Cooper commended MySpace for its willingness to make its site safer, calling it an industry leader and urging other social networks to adopt the safety principles in today’s agreement.

The agreement culminates nearly two years of discussions between MySpace and the Attorneys General. The Attorneys General were led by North Carolina Attorney General Roy Cooper and Connecticut Attorney General Richard Blumenthal, co-chairmen of the multistate group’s Executive Committee consisting of Connecticut, North Carolina, Georgia, Idaho, Massachusetts, Mississippi, New Hampshire, Ohio, Pennsylvania, Virginia and the District of Columbia. Attorneys General from 49 states and the District of Columbia signed the agreement.

Under the agreement, MySpace, with support from the attorneys general, will create and lead an Internet Safety Technical Task Force to explore and develop age and identity verification tools for social networking web sites. MySpace will invite other social networking sites, age and identify verification experts, child protection groups and technology companies to participate in the task force.

The task force will report back to the attorneys general every three months and issue a formal report with findings and recommendations at the end of 2008.

MySpace also will hire a contractor to compile a registry of email addresses provided by parents who want to restrict their child's access to the site. MySpace will bar anyone using a submitted email address from signing in or creating a profile.

MySpace also agreed to work to:

- Strengthen software identifying underage users;
- Retain a contractor to better identify and expunge inappropriate images;
- Obtain and constantly update a list of pornographic web sites and regularly sever any links between them and MySpace;
- Implement changes making it harder for adults to contact children;
- Dedicate meaningful resources to educating children and parents about on-line safety;
- Provide a way to report abuse on every page that contains content, consider adopting a common mechanism to report abuse, and respond quickly to abuse reports;
- Create a closed "high school" section for users under 18.

"This agreement tackles some of the most risky elements of social networking, but we must do even more to keep kids safe online," said Cooper. "We'll keep pushing to find child predators and put them behind bars, and well keep urging parents to pay attention to what their kids are doing on the computer."

###

JOINT STATEMENT ON KEY PRINCIPLES OF SOCIAL NETWORKING SITES SAFETY

MySpace and the Attorneys General have discussed social networking sites safety measures with great vigor over several months. MySpace and the Attorneys General agree that social networking sites are a powerful communications tool that provides people with great social benefits. However, like all communication tools, social networking sites can be misused as a means to commit crimes against minors and can allow minors to gain access to content that may be inappropriate for them.

MySpace and the Attorneys General recognize that millions of minors across the world access the Internet each day, and that many of these minors create social networking profiles on MySpace and other social networking sites. Based on recommendations MySpace received from the Attorneys General and online safety advocates, and as a result of its internal safety and engineering teams, MySpace has implemented technologies and procedures to help prevent children under 14 from using MySpace and to help protect minors age 14 and above from exposure to inappropriate content and unwanted contact by adults. The Attorneys General commend MySpace for its efforts to address these issues. They also call upon other social networking services to adopt these principles.

MySpace and the Attorneys General agree that additional ways to protect children should be developed. This effort is important as a policy matter and as a business matter.

PRINCIPLE: Providing children with a safer social networking experience is a primary objective for operators of social networking sites.

I. ONLINE SAFETY TOOLS

PRINCIPLE: Technology and other tools that empower parents, educators and children are a necessary element of a safer online experience for children.

PRINCIPLE: Online safety tools, including online identity authentication technologies, are important and must be robust and effective in creating a safer online experience, and must meet the particular needs of individual Web sites.

- MySpace will organize, with support of the Attorneys General, an industry-wide Internet Safety Technical Task Force (“Task Force”) devoted to finding and developing such online safety tools with a focus on finding and developing online identity authentication tools. This Task Force will include Internet businesses, identity authentication experts, non-profit organizations, and technology companies.
- The Task Force will establish specific and objective criteria that will be utilized to evaluate existing and new technology safety solutions.

- MySpace and other members of the Task Force will provide adequate resources to ensure that all reasonable efforts are made to explore and develop identity authentication technologies.
- News Corporation will designate a senior executive to work with the Task Force.
- The Task Force will provide the Executive Committee of the Attorneys General Social Networking Working Group (“Executive Committee”) with quarterly reports of its efforts and presentation of a formal report by the end of 2008. The Executive Committee will have continuing access to the Task Force and the designated senior executive of News Corporation.

II. DESIGN AND FUNCTIONALITY CHANGES

PRINCIPLE: Development of effective Web site design and functionality improvements to protect children from inappropriate adult contacts and content must be an ongoing effort.

- MySpace and the Attorneys General share the goal of designing and implementing technologies and features that will make MySpace safer for its users, particularly minors. More specifically, their shared goals include designing and implementing technologies and features that will (1) prevent underage users from accessing the site; (2) protect minors from inappropriate contact; (3) protect minors from inappropriate content; and (4) provide safety tools for all MySpace users.
- The Attorneys General acknowledge that MySpace is seeking to address these goals by (1) implementing the design and functionality initiatives described in Appendix A; and (2) working to implement the design and functionality initiatives described in Appendix B.
- MySpace and the Attorneys General will meet on a regular basis to discuss in good faith design and functionality improvements relevant to protecting minors using the Web site.

III. EDUCATION AND TOOLS FOR PARENTS, EDUCATORS, AND CHILDREN

PRINCIPLE: Educating parents, educators and children about safe and responsible social networking site use is also a necessary part of a safe Internet experience for children.

- MySpace will continue to dedicate meaningful resources to convey information to help parents and educators protect children and help younger users enjoy a safer experience on MySpace. These efforts will include MySpace's plan to engage in public service announcements, develop free parental monitoring software, and explore the establishment of a children's email registry.
- MySpace shall use its best efforts to acknowledge consumer reports or complaints received via its abuse reporting mechanisms within 24 hours of receiving such report or complaint. Within 72 hours of receiving a complaint or report from a consumer regarding inappropriate content or activity on the site, MySpace will report to the consumer the steps it has taken to address the complaint.
- For a two (2) year period MySpace shall retain an Independent Examiner, at MySpace's expense, who shall be approved by the Executive Committee. The Independent Examiner shall evaluate and examine MySpace's handling of these consumer complaints and shall prepare bi-annual reports to the Executive Committee concerning MySpace's consumer complaint handling and response procedures, as provided above.

IV. LAW ENFORCEMENT COOPERATION

PRINCIPLE: Social networking site operators and law enforcement officials must work together to deter and prosecute criminals misusing the Internet.

- MySpace and the Attorneys General will work together to support initiatives that will enhance the ability of law enforcement officials to investigate and prosecute Internet crimes.
- MySpace and the Attorneys General will continue to work together to make sure that law enforcement officials can act quickly to investigate and prosecute criminal conduct identified on MySpace.
- MySpace has established a 24-hour hotline to respond to law enforcement inquiries. In addition, News Corporation will assign a liaison to address complaints about MySpace received from the Attorneys General. MySpace will provide a report on the status of its response to any such complaint within 72 hours of receipt by the liaison.

Agreed to and accepted on January 14th, 2008:

Mike Angus
EVP, General Counsel, Fox Interactive Media

Richard Blumenthal
Attorney General of Connecticut

Peter Nickles
Interim Attorney General of D.C.

Lawrence Wasden
Attorney General of Idaho

Jim Hood
Attorney General of Mississippi

Marc Dann
Attorney General of Ohio

Robert McDonnell
Attorney General of Virginia

Roy Cooper
Attorney General of North Carolina

Thurbert E. Baker
Attorney General of Georgia

Martha Coakley
Attorney General of Massachusetts

Kelly Ayotte
Attorney General of New Hampshire

Tom Corbett
Attorney General of Pennsylvania

Troy King
Attorney General of Alabama

Talis Colberg
Attorney General of Alaska

Terry Goddard
Attorney General of Arizona

Dustin McDaniel
Attorney General of Arkansas

John Suthers
Attorney General of Colorado

Joseph R. Biden III
Attorney General of Delaware

Bill McCollum
Attorney General of Florida

Mark J. Bennett
Attorney General of Hawaii

Lisa Madigan
Attorney General of Illinois

Stephen Carter
Attorney General of Indiana

Tom Miller
Attorney General of Iowa

Paul Morrison
Attorney General of Kansas

Jack Conway
Attorney General of Kentucky

Charles C. Fóti, Jr.
Attorney General of Louisiana

G. Steven Rowe
Attorney General of Maine

Douglas Gansler
Attorney General of Maryland

Michael A. Cox
Attorney General of Michigan

Lori Swanson
Attorney General of Minnesota

Jeremiah W. Nixon
Attorney General of Missouri

Mike McGrath
Attorney General of Montana

Jón Bruning
Attorney General of Nebraska

Catherine Cortez Masto
Attorney General of Nevada

Anne Milgram
Attorney General of New Jersey

Gary King
Attorney General of New Mexico

Andrew M. Cuomo
Attorney General of New York

Wayne Stenehjem
Attorney General of North Dakota

W.A. Drew Edmondson
Attorney General of Oklahoma

Hardy Myers
Attorney General of Oregon

Patrick C. Lynch
Attorney General of Rhode Island

Henry McMaster
Attorney General of South Carolina

Lawrence E. Long
Attorney General of South Dakota

Robert E. Cooper, Jr.
Attorney General of Tennessee

Mark L. Shurtleff
Attorney General of Utah

William H. Sorrell
Attorney General of Vermont

Rob McKenna
Attorney General of Washington

Darrell V. McGraw, Jr.
Attorney General of West Virginia

J.B. Van Hollen
Attorney General of Wisconsin

Bruce Salzburg
Attorney General of Wyoming

APPENDIX A: DESIGN AND FUNCTIONALITY CHANGES

Preventing Underage Users

1. Browse function - limit to 68 years and below.
2. MySpace will implement “age locking” for existing profiles such that members will be allowed to change their ages only once above or below the 18 year old threshold. Once changed across this threshold, under 18 members will be locked into the age they provided while 18 and older members will be able to make changes to their age as long as they remain above the 18 threshold. MySpace will implement “age locking” for new profiles such that under 18 members will be locked into the age they provide at sign-up while 18 and older members will be able to make changes to their age as long as they remain above the 18 threshold.

Protecting Younger Users from Inappropriate Contact

1. Users able to restrict friend requests to only those who know their email address or last name.
2. “Friend only” group invite mandatory for 14 and 15 year olds.
3. “Friend only” group invite by default for 16 and 17 years olds.
4. Users under 18 can block all users over 18 from contacting them or viewing their profile.
5. Users over 18 will be limited to search in the school section only for high school students graduating in the current or upcoming year.
6. Users over 18 may designate their profiles as private to users under 18, and users under 18 may designate their profiles as private to users over 18.
7. Limit search engine ability to crawl all private profiles.
8. Users under 18 cannot designate themselves as swingers.
9. Users under 16 are automatically assigned a private profile.
10. Users over 18 cannot browse for users under 18.
11. A user cannot browse for users under 16.
12. Users over 18 cannot add users under 16 as friends unless they know the under 16 user's last name or email address.

13. Personally identifiable information removed upon discovery.
14. Users under 18 cannot browse for swingers.
15. MySpace will not allow unregistered visitors to the site to view any search results related to mature areas of the site, profiles that are private to under 18s, or other groups and forums geared toward sexual activity and mature content.
16. MySpace will change the default for under 18 members to require approval for all profile comments.
17. MySpace will remove the ability for under 18 members to browse the following categories: relationship status, “here for”, body type, height, smoke, drink, orientation and income.
18. If users under 16 override their privacy settings, they are still only viewable by other users under 18.
19. When user posts images, they will receive a note including IP address of the computer that uploaded the image.
20. Add sender URL in mail for private messages.
21. Locate underage users (searching specific keywords, reviewing groups and forums, and browsing certain age ranges).
22. Profiles of Registered Sex Offenders identified through Sentinel SAFE technology are reviewed and, once confirmed, are removed from the site. The associated data are preserved for law enforcement.

Protecting Younger Users from Inappropriate Content

1. Implementation of image policy for hosted images that employs hashing technology to prevent inappropriate image uploads.
2. Expand flag spam/abuse to allow categorization of flagged message.
3. Expand “Report Image” functionality to include a drop down menu that provides members with greater specificity on why they are reporting image. Categories to include Pornography, Cyberbullying, and Unauthorized Use.
4. Under 18s/under 21s cannot access tobacco/alcohol advertisements.
5. MySpace and Attorneys General commit to discuss with Google the need to cease directing age inappropriate linked advertisements to minors.

6. Events may be designated for all ages, for 18 + or for 21+.
7. MySpace will notify users whose profiles are deleted for Terms of Service Violations.
8. Groups reviewed for incest, hate speech or youth sex subjects with violators removed from site.
9. Members determined to be under 18 to be removed from mature Groups.
10. Posts determined to be made to mature Groups by under 18 members to be removed.
11. Any mature Groups determined to be created by under 18 members will be removed entirely and the user accounts may be deleted for violating the Terms of Service.
12. Users under 18 to be denied access to Romance & Relationships Forum and Groups.
13. Users under 18 will not have access to inappropriate parts of Classifieds (dating, casting calls).
14. Members may request to label Groups they create as mature.
15. Flagged Groups are reviewed and categorized by MySpace staff.
16. Members under 18 and non-registered users may not enter or view a Group page that has been designated as mature.
17. MySpace hired a Safety Product Manager.
18. Smoking/Drinking preferences blocked for under 18s/under 21s.
19. User accounts promptly deleted for uploading child pornographic images and/or videos and referred to NCMEC.
20. MySpace does not tolerate pornography on its site, and users determined to have uploaded pornographic images and/or videos flagrantly and/or repeatedly will have their accounts deleted.

Providing Safety Tools For All Members

1. All users may set profile to private.
2. All users can pre-approve all comments before being posted.

3. Users can block another user from contacting them.
4. Users can conceal their “online now” status.
5. Users can prevent forwarding of their images to other sites.
6. MySpace adds “Report Abuse” button to Email, Video, and Forums.
7. Users over 18 can block under 18 users from contacting them or viewing their profiles.
8. All users can allow only those users whom they have proactively added to their Contact List to see when they are on IM and to contact them.
9. “Safety Tips” Available on every page of MySpace.
10. “Safety Tips” Appear on registration page for anyone under 18.
11. Users under 18 must affirmatively consent that user has reviewed the Safety Tips prior to registration. MySpace will require under 18 members to scroll through the complete Safety Tips upon registration. MySpace will also require under 18 members to review the Safety Tips on an annual basis.
12. Additional warning posted to users under 18 regarding disclosure of personal information upon registration.
13. Safety Tips are posted in the “mail” area of all existing users under 18.
14. Safety Tips contain resources for Internet Safety including FTC Tips.
15. Phishing warning added to Safety Tips.
16. Safety Tips for Parents provides links to free blocking software.
17. Parent able to remove child's profile through the ParentCare Hotline and ParentCare Email.
18. MySpace will have “Tom” become a messenger to deliver Safety Tips to minors on MySpace.
19. All users under 18 receive security warnings before posting content.

APPENDIX B: DESIGN AND FUNCTIONALITY INITIATIVES

MySpace will continue to research and develop online safety tools. Based on recommendations MySpace received from the Attorneys General and online safety advocates, and as a result of the work of its internal safety and engineering teams, MySpace's current plans include the following initiatives:

Limiting MySpace Membership to Users 14 and Over

1. Engage a third-party to build and host a registry of email addresses for children under 18. Parents would register their children if they did not want them to have access to MySpace or any other social networking site that uses the registry. A child whose information matches the registry would not be able to register for MySpace membership.
2. Strengthen the algorithm that identifies underage users.

Protecting Minors from Unwanted Contacts by Adults

1. Change the default setting for 16-17 year olds' profiles from "public" to "private."
2. Create a closed high school section for users under 18. The "private" profile of a 16/17 year old will be viewable only by his/her "friends" and other students from that high school who have been vouched for by another such student. Students attending the same high school will be able to "Browse" for each other.

Protecting Minors from Exposure to Inappropriate Content

1. MySpace will review models for a common abuse reporting icon (including the New Jersey Attorney General's "Report Abuse" icon). If MySpace determines that a common icon is workable and will improve user safety, it may substitute the common icon for the current report abuse icon MySpace places on each member profile.
2. Obtain a list of adult (porn) Web sites on an ongoing basis and sever all links to those sites from MySpace.
3. Demand that adult entertainment industry performers set their profiles to block access to all under 18 users.
4. Remove all under 18 users from profiles of identified adult entertainment industry performers.
5. Retain image review vendor(s) that can effectively and efficiently identify inappropriate content so it can be removed from the site more expeditiously.

6. Investigate the use of an additional image review vendor to provide automated analysis of images to help prioritize images for human review.
7. MySpace will (1) develop and/or use existing technology such as textual searching; and (2) provide increased staffing, if appropriate, in order to more efficiently and effectively review and categorize content in “Groups.” MySpace will update the Attorneys General concerning its efforts to develop and/or use textual searching on a quarterly basis. Upon implementation of textual searching, the Attorneys General will review its efficacy with respect to “Groups” for a period of 18 months.

APPENDIX B:
Task Force Project Plan

Internet Safety Technical Task Force Project Plan

June 27, 2008

I. Background.

The Internet Safety Technical Task Force has been convened in response to a joint statement between MySpace and 49 State Attorneys General. The agreement, announced on January 14, 2008, reads, in part:

“MySpace will organize, with support of the Attorneys General, an industry-wide Internet Safety Technical Task Force (“Task Force”) devoted to finding ... online safety tools with a focus on finding ... online identity authentication tools. This Task Force will include Internet businesses, identity authentication experts, non-profit organizations, and technology companies. ... The Task Force will establish specific and objective criteria that will be utilized to evaluate existing and new technology safety solutions.”

II. Scope.

The scope of the Task Force’s inquiry is to consider those technologies that industry and end users can use to keep children safe on the Internet. The problems that the Task Force is working on are large and complex; their boundaries are hard to define. The key questions that we seek to answer are:

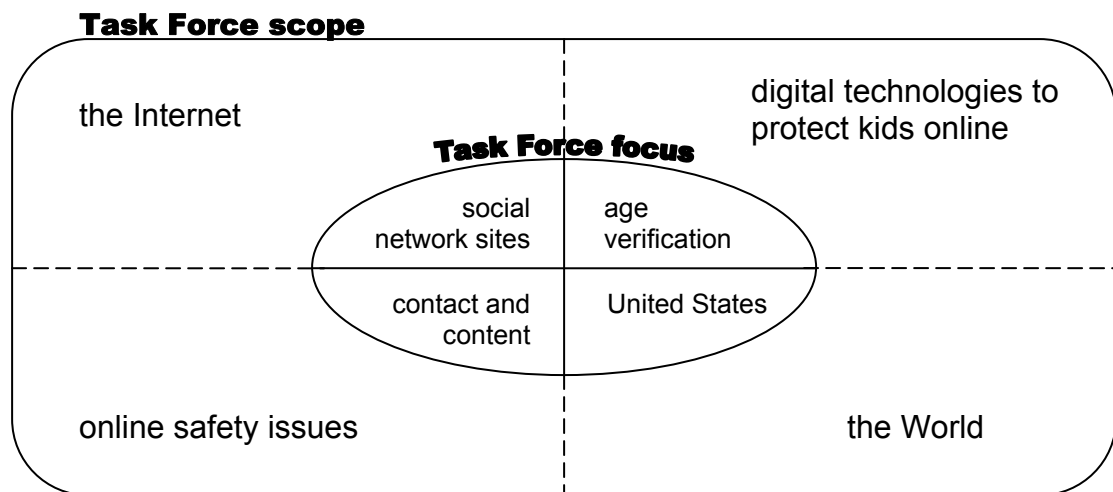
1. Are there technologies that can limit harmful contact between children and other people?
2. Are there technologies that can limit the ability of children to access and produce inappropriate and/or illegal content online?
3. Are there technologies that can be used to empower parents to have more control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

Within each of these broad topic areas, the Task Force will seek to determine 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 inquiry will address all minors (i.e., people under the age of 18), but the Task Force will seek where possible to tailor its recommendations to more refined subsets in age.

The Task Force is chartered specifically to assess age verification technology as a means to reduce the harmful contact and content experienced by children using social network sites in the United States. Popular media have highlighted privacy and safety concerns that arise when children use social network sites¹, but the nature of the danger

¹ danah m. boyd and Nicole. B. Ellison, Social Network Sites: Definition, History, and Scholarship, *Journal of Computer-Mediated Communication*, 13(1), article 11, 2007, <http://jcmc.indiana.edu/vol13/issue1/boyd.ellison.html>.

to children remains the topic of ongoing research that places the problem in a broader social, technological, and geographical context. Recognizing this broader setting, the Task Force has the flexibility to consider harmful contact and harmful content in the context of online safety issues in general. Likewise, while focusing on harms that occur in social network sites, the Task Force will not ignore the broader environment of the Internet as a whole. Age verification technology will be assessed in the context of other digital technologies that protect children online. Finally, the Task Force will consider the problem of child safety on the Internet in an international context, with emphasis on issues arising in the United States.



The Task Force acknowledges that, given limited time and resources, its work will represent a series of next steps, but not final answers, to each of these problems. The Task Force acknowledges also that while we can list a number of problems, not every aspect of the problems of child safety online can be addressed in full during this process. The Task Force notes that much work has been done in these areas and every effort will be made to build off of previous efforts.

In assessing and describing the possible technical solutions, the Task Force will take into account the feasibility and cost of technology solutions. In the final report, the Task Force will place these technological approaches into a context that also includes related public policy issues. The final report will also include “specific and objective criteria that will be utilized to evaluate existing and new technology safety solutions,” as set forth in the joint statement.

III. Structure.

The Task Force is comprised of those companies, NGOs, and academic groups that have agreed to join at MySpace’s invitation. The Task Force is directed by John Palfrey, danah boyd, and Dena Sacco, all of the Berkman Center for Internet & Society. The work of the Task Force will be supported by a Research Advisory Board and a Technical Advisory

Board. The purpose of these supporting advisory boards is to enable the Task Force to accept input from experts on these topics who are not members of the Task Force. The Task Force will also include informal subcommittees comprised of Task Force members with a particular interest or expertise in the three issue areas.

The Research Advisory Board (RAB) will be chaired by the Berkman Center's danah boyd and will be comprised of scholars, professional researchers, and organizations investigating online safety-related issues through large scale data collection. Examples of this group include the UNH Crimes Against Children Research Center, Michele Ybarra, and the Pew and the Internet and American Life Project. The RAB will work with scholars to assess existing threats to youth online safety to determine which are the most common, which are the most harmful, and which potentially can be addressed by technological solutions. It will aggregate what is known about the state of child safety online and the effectiveness of different legal, technological, and educational approaches to addressing it. It will take into account the existing research in these areas, as well as evaluate what additional research would be most helpful. Ultimately, the Board will produce a report for the Task Force that describes the state of the research. Pending funding, the Board will recommend that the Task Force commission additional research as appropriate. Both the report and any future research proposals will be presented to the Task Force and be referenced in the Task Force's final report. Additionally, both will be made publicly available.

The Technical Advisory Board will be chaired by Laura DeBonis and will focus on the range of possible technological solutions to the problems of youth online safety, including identity authentication tools, filtering, monitoring, and scanning and searching. The Technical Advisory Board (TAB) will consider the potential solutions introduced by the Task Force, those that emerge through the Research Advisory Board, and those introduced by the public. It will develop technical criteria for assessing the various solutions. The TAB will reach out to a range of technologists who understand and can evaluate the different available technological approaches to online safety. The Board will accept proposals from a wide variety of vendors and will write a report for the Task Force addressing the different potential solutions. As with the Research Advisory Board, the Berkman Center will convene this ad hoc group prior to the June 20 meeting in Cambridge. It will be comprised of financially disinterested parties who are open to technological solutions to the Internet Safety concerns facing children.

Task Force members are each encouraged to join a subcommittee of the Task Force organized around each of the three key questions under consideration. Each of these subcommittees will be empowered to determine the most pressing issues within each issue area, to assess previous work in each of these areas, to come up with lists of technologies and research to be considered by others, and to propose topics to the Berkman Center team for the final report. The Berkman Center will support conference calls or other means of subcommittee self-organization.

IV. Systems.

A. Reports.

As set forth in the January, 2008 Agreement between the Attorneys General and MySpace, the Task Force owes quarterly reports to the Attorneys General, as well as a Final

Report on December 31, 2008. The Berkman Center will draft the reports. The first quarterly report was submitted to the Attorneys General in April. The reports will be circulated to Task Force members in advance of sending them to the Attorneys General for comment. The Berkman Center team will consider all comments from Task Force members.

B. Meetings.

To undertake its work, the Task Force as a whole will hold a series of day-long meetings. Four of the meetings will be open only to Task Force members and those the Task Force invites to make presentations and/or to observe. Each meeting will involve a segment that is open for the public to participate. We will publish minutes from each Task Force meeting on the web. The meetings will take place on the following dates:

March 12, 2008 (organizational meeting, in Washington, DC)
April 30, 2008 (first full meeting, in Washington, DC)
June 20, 2008 (second full meeting, in Cambridge, MA)
September 23, 2008 (public session in Cambridge, MA)
September 24, 2008 (third full meeting, in Cambridge, MA)
November 19, 2008 (fourth full meeting, in Washington, DC)

The open public meeting on September 24, 2008 is intended to provide a forum for all interested parties to present their views. The Berkman Center will solicit short written submissions from those who intend to attend the open meeting, in order to better keep track of attendees and their input, and will make those submissions available on the Task Force's public web site.

Both the Research Advisory Board and the Technological Advisory Board will likely hold a few conference calls as needed to facilitate their work. They will report their progress to the Task Force formally at the meetings and informally as appropriate.

The Task Force may convene an additional meeting or calls to review technologies and the draft report close to the end of the calendar year.

C. Website and Online Workspace.

The Task Force has a public-facing website that includes a description of the Task Force, contact information for the Berkman Center team, and an FAQ section. The Berkman Center has created a private Listserv for the Task Force as a whole and will do so for each of the Advisory Boards. Postings to the Task Force's listserv are considered off the record and are not to be forwarded to those not on the list.

V. Communications.

The Berkman Center will act as primary contact for the Task Force, both for press inquiries and for requests for involvement by interested parties. Task Force Members are welcome to forward press inquiries to the Berkman Center as appropriate. We ask that you copy all requests from interested parties seeking involvement in the work of the Task Force to us, so that we can act as a central clearinghouse for these requests and so that interested parties are not left out of invitations to participate.

VI. Intellectual Property.

The Task Force has developed and posted an Intellectual Property Policy² to safeguard the IP rights of members and non-member contributors. It emphasizes that Task Force members are under no obligation to protect the confidentiality of submissions to the Task Force.

² Berkman Center for Internet & Society, Intellectual Property Policy for the Internet Safety Technical Task Force, June 2008, <http://cyber.law.harvard.edu/research/isttf/ippolicy>.

APPENDIX C:

**Research Advisory Board
Literature Review**

Online Threats to Youth: Solicitation, Harassment, and Problematic Content

Literature Review Prepared for the Internet Safety Technical Task Force
<http://cyber.law.harvard.edu/research/isttf>

Andrew Schrock and danah boyd
Berkman Center for Internet & Society
Harvard University

Research Advisory Board Members involved in shaping this document:

- *David Finkelhor*, Director of University of New Hampshire's Crimes Against Children Research Center
- *Sameer Hinduja*, Assistant Professor of Criminology and Criminal Justice at Florida Atlantic University
- *Amanda Lenhart*, Senior Research Specialist at Pew Internet and American Life Project
- *Kimberly Mitchell*, Research Assistant Professor at University of New Hampshire's Crimes Against Children Research Center
- *Justin Patchin*, Assistant Professor at University of Wisconsin–Eau Claire
- *Larry Rosen*, Professor of Psychology at California State University, Dominguez Hills
- *Janis Wolak*, Research Assistant Professor at University of New Hampshire's Crimes Against Children Research Center
- *Michele Ybarra*, President of Internet Solutions for Kids

Table of Contents

1. Introduction.....	4
1.1. Scope.....	6
1.2. A Note on Methodology and Interpretation.....	7
1.3. Youths Facing Risks.....	10
1.4. Youth Perpetrators.....	11
1.5. Adult Perpetrators.....	11
2. Sexual Solicitation and Internet-Initiated Offline Encounters.....	13
2.1. Solicitation.....	14
2.2. Offline Contact.....	16
2.3. Victims.....	18
2.4. Perpetrators.....	19
3. Online Harassment and Cyberbullying.....	21
3.1. Victims.....	22
3.2. Perpetrators.....	24
3.3. Overlaps in Victimization and Perpetration.....	25
3.4. Offline Connections.....	26
3.5. Connections to Solicitation.....	27
4. Exposure to Problematic Content.....	28
4.1. Pornography.....	28
4.2. Violent Content.....	30
4.3. Other Problematic Content.....	31
5. Child Pornography.....	34
5.1. Child Pornography Offenders.....	35
5.2. Child Pornography and Sexual Solicitation.....	35
6. Risk Factors.....	38
6.1. Online Contact with Strangers.....	38
6.2. Posting of Personal Information.....	39
6.3. Sharing of Passwords.....	40
6.4. Depression, Abuse, and Substances.....	41
6.5. Poor Home Environment.....	42

7. Genres of Social Media.....	45
7.1. Chatrooms and Instant Messaging.....	45
7.2. Blogging.....	46
7.3. Social Network Sites.....	47
7.4. Multiplayer Online Games and Environments	48
7.5. Multimedia Communications.....	50
8. Future Research	51
8.1. Minor-minor Solicitation and Sexual Relations	51
8.2. Problematic Youth Generated Content	52
8.3. Impact on Minority Groups	53
8.4. Photographs and Video in Online Harassment and Solicitation.....	54
8.5. Intersection of Different Mobile and Internet-based Technologies	54
8.6. Continued Research, New Methodologies, and Conceptual Clarity.....	55
9. Appendix A: Understanding Research Methodologies.....	57
9.1. Samplings.....	57
9.2. Response Rates	58
9.3. Prevalence	59
9.4. Sources of Bias	60
9.5. Constructs	60
9.6. Question Wording.....	61
9.7. Causality and Complexity.....	61
9.8. Qualitative Methodologies.....	62
9.9. Funding Sources.....	62
9.10. Underreporting of Incidents.....	63
10. References.....	64

1. Introduction

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 (Marwick 2008). 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 not risks, but it is important to ask critical questions in order to get an accurate picture of the online environment and the risks that youth face there. This literature review 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.

1.1. Creation

This document was primarily 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 Research Advisory Board (RAB) and co-director of the Internet Safety Technical Task Force. This document has been vetted for accuracy and integrity by those contributors to the Research Advisory Board listed at the beginning of the document.

Researchers and scholars from the United States whose work is relevant to the Task Force were invited to contribute to the efforts of the RAB. 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 this document by providing citations, critiques of the review, and otherwise expressing feedback. The RAB intended the review to be as inclusive as possible. No researcher was excluded based on their findings or opinions. Those who contributed to this process who wished to be identified are listed at the top of this document. 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.

This document was created to help 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 look at the data. We believe 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. We do not present potential solutions, because these are outside the scope of this document, but we believe that solutions that are introduced should be measured as to their actual effectiveness in addressing the risks youth face, instead of in terms of adult perception of their effectiveness at solving perceived risks.

Parallel efforts are underway in the European Union, where scholars have recently authored a document that compares the risks and opportunities youth face across Europe in different media environments (Hasebrink et al. 2008). This literature review provides a complementary American perspective.

1.2. Scope

The goal of this literature review is to map out what is currently understood about the intersections of youth, risk, and social media. We framed this review around the most prevalent risks youth face when online: harassment, solicitation, and exposure to problematic content. We

address risks youth face offline, such as unmediated sexual solicitation, schoolyard bullying, substance abuse, and family problems, primarily to contextualize online 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 there are limited numbers of large-scale studies, 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 felt 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 or 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 Internet Safety Technical Task Force had the best data available.

A legalistic discussion is outside of the scope of this document. We periodically use such references for context, but our review primarily focuses on psychological and sociological approaches to youth and risk. Many of the online contact threats to youth that we address (including sexual solicitation and online harassment) are not prosecutable crimes in all regions in the United States. Internet solicitation of a young adolescent by an adult is a prosecutable offense in some states (depending on the exact ages of the parties), and in most states if it leads to an offline statutory rape (Hines and Finkelhor 2007) or sexual assault. Other forms of online contact, such as online harassment between two minors, ride the line of legality.

Youth encounter a variety of problematic content online, including adult pornography, violent movies, and violent video games. This material is typically not illegal to distribute to minors, or for minors to possess, although it is considered to be age-inappropriate and age restrictions may exist on purchasing it. Efforts to identify what is considered harmful or obscene are judged by “contemporary community standards,” which are difficult to define. Pornographic content depicting minors (“child pornography”), by comparison, is illegal to possess or distribute

in the United States (see: 102 Stat. 4485, 18 U.S.C. §2251 et seq. [2006]) and is universally condemned.¹

Efforts of researchers worldwide to understand and document the risks youth face have been invaluable in furthering our understanding of Internet threats to minors. But in many ways, we still know very little about the details of these complex threats and how they are related. For instance, the relationship between minor-to-minor sexual solicitation and minor-to-minor harassment is only now being examined (Ybarra et al. 2007b). There are also gaps in the literature, which we discuss in section 8. For example, little is known about the problematic content that youth produce and distribute, such as videos of fights or pornographic images of themselves, and emerging technologies like the mobile phone have not yet been considered in depth. Finally, although multiple studies are underway, there is still a need for more large-scale quantitative research, particularly nationwide longitudinal surveys and studies that include data collected by law enforcement. Meaningful qualitative research on victims and offenders is similarly needed to enhance our understanding of threats to youth online.

1.3. A Note on Methodology and Interpretation

Research into youth, risks, and social media stems from a wide variety of different methodological approaches. The studies discussed in this review take different approaches, although they all have limitations and biases. Some research questions are better answered by a certain methodology or research design. For example, questions that begin with “why” or “how” are often more adequately addressed through qualitative approaches than quantitative ones. Qualitative scholarship is better suited for providing a topological map of the issues, and quantitative scholarship can account for frequency, correlation, and the interplay of variables. Many quantitative studies discussed in this review reference and build on qualitative findings, and several utilize “mixed-methods” research with both quantitative and qualitative dimensions.

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

¹ The international situation is much different, as more than half of countries have inadequate laws governing the creation and distribution of child pornography (International Centre for Missing & Exploited Children 2006). This legal perspective—particularly the state of laws worldwide—is important, but outside of the purview of this review.

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 is involved that involves both. For those who are not familiar with different research methodologies, Appendix A provides some of the major structural issues one should be familiar with when considering the strengths and weaknesses of studies in this review.

Although research in this area is still quite new, many of the studies presented here come to similar conclusions using different participant groups and analytic approaches. When this is not the case, we highlight the issue and provide possible explanations for the discrepancy. Most often, discrepancies can be explained by understanding methodological differences, such as in research instrumentation, data collection, and sampling frame.

Research in this area is frequently misunderstood and even more frequently mischaracterized. This is unfortunate, because the actual threats youth face are often different than the threats most people imagine. More problematically, media coverage has regularly mischaracterized research in this area, leading 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 mentioned in the following discussion, other peers and young adults account for 90%–94% of solicitations where 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). Researchers also do not use the concept of “solicitation” to refer specifically to messages intended to persuade a minor into sexual activity; it more generally refers to communications of a sexual nature, including sexual harassment and flirting.

Misperception of these findings perpetuates myths that distract the public from solving the actual problems youth face.

The purpose of this literature review is to move beyond fears or myths and paint an accurate and data-centric portrait of what risks youth are truly facing. Although fears of potential dangers are pervasive, the research presented here documents the known prevalence and frequency of Internet harm. Threats involving the Internet have not overtaken other harmful issues that youth encounter. For instance, although pervasive and frequently reported in the media (Potter and Potter 2001), Internet sex crimes against minors have not overtaken the number of unmediated sex crimes against minors (Wolak et al. 2003b), nor have they contributed to a rise in such crimes. This situation may seem at odds with the large number of reports made of Internet crimes against youth—in 2006, CyberTipline (a congressionally mandated system for reporting child crimes) received 62,365 reports of child pornography, 1087 of child prostitution, 564 of child sex tourism, 2145 of child sexual abuse, and 6334 reports of online enticement of children for sexual acts (National Center for Missing and Exploited Children 2006). Yet the increased popularity of the Internet in the United States has not been correlated with an overall increase in reported sexual offenses; overall sexual offenses against children have gone steadily down in the last 18 years (National Center for Missing and Exploited Children 2006). State-reported statistics show a –53% change in reports of sexual offenses against children from 1992 to 2006 (Calpin 2006; Finkelhor and Jones 2008), which Finkelhor (2008) argues is both significant and real. Furthermore, sex crimes against youth not involving the Internet outweigh those that do; Internet-initiated statutory relationships are greatly outnumbered by ones initiated offline (Snyder and Sickmund 2006; Wolak et al. 2003b) and the majority of sexual molestations are perpetrated primarily by those the victim knows offline, mainly by family members or acquaintances (Snyder and Sickmund 2006). This appears to be partly true of Internet-initiated sexual offenses as well, as a considerable percentage (44%) of Internet sexual offenders known to youth victims were family members (Mitchell et al. 2005b).

When it comes to harmful content, studies show that the Internet increases children’s risk of “unwanted” (accidental or inadvertent) exposure to sexual material (Wolak et al. 2006). It is debatable whether or not this type of encounter is new as a result of the Internet. On the topic of sexual solicitation, studies show that things are either improving or have been shown to not be as prevalent and distressing to minors as initially anticipated. Between 2001 and 2005, the

proportion of youth receiving unwanted Internet sexual solicitations went down (Wolak et al. 2006), although this decline was only seen among white youth and those living in higher-income households (Mitchell et al. 2007a). It was also discovered that the majority of cases of sexual solicitation involved adolescents, while instances of prepubescent children being solicited online are nearly nonexistent (Wolak et al. 2008b).

1.4. Youths Facing Risks

This document examines online risks to *youth*, which is synonymous with *minors* and is used to refer to individuals under the age of 18. *Adolescents* or *teenagers* are used to refer to youth aged 13 to 17 years old (inclusive), unless stated otherwise. *Children* are considered to be prepubescent youth aged 0 to 12 years old (although a minority of youth in this age range has reached puberty). Several studies are able to claim a representative, national sampling of youth in the United States, but the majority of studies are conducted with smaller groups, such as students in a particular school system or set of classes. Not all studies examine the same range of ages; therefore, the ages of study participants will be provided in our discussion.

The public commonly views children as more vulnerable than adolescents when it comes to Internet safety. In reality, there is a spectrum of sexual development through childhood (Bancroft 2003), and by adolescence, it is generally recognized that a curiosity about sexualized topics is developmentally normative (Levine 2002). Contrary to expectations and press coverage, adolescents or teenagers are more at risk for many threats, such as online solicitation and grooming (Beebe et al. 2004; Mitchell et al. 2001, 2007b; Wolak et al. 2004, 2008b; Ybarra et al. 2007b), and are more likely to search out pornographic material online than prepubescent children (Peter and Valkenburg 2006; Wolak et al. 2007b; Ybarra and Mitchell 2005: 473). Even unwanted exposure occurs more among older youth (Snyder and Sickmund 2006; Wolak et al. 2007b). Online harassment appears less frequently among early adolescents (Lenhart 2007; Ybarra and Mitchell 2004a) and children (McQuade and Sampat 2008). It is seemingly highest in mid-adolescence, around 13–14 years of age, (Kowalski and Limber 2007; Lenhart 2007; McQuade and Sampat 2008; Slonje and Smith 2008; Williams and Guerra 2007).

Even apart from age differences, some youth are more at risk than other youth. Race is generally not a significant factor in these crimes, such as cyberbullying and online harassment (Hinduja and Patchin 2009; Nansel et al. 2001; Ybarra et al. 2007a). Girls tend to be more at risk

for being victimized by online solicitation (Wolak et al. 2006) and harassment (Agatston et al. 2007; DeHue et al. 2008; Kowalski and Limber 2007; Lenhart 2007; Li 2005, 2006, 2007b; Smith et al. 2008). Boys generally see more pornography (Cameron et al. 2005; Flood 2007; Lenhart et al. 2001; Nosko et al. 2007; Peter and Valkenburg 2006; Sabina et al. 2008; Stahl and Fritz 1999; Wolak et al. 2007b; Ybarra and Mitchell 2005), particularly that which they seek out. Online youth victims also have been found to have a myriad of other problems, including depression (Ybarra et al. 2004) and offline victimization (Finkelhor 2008; Mitchell et al. 2007a).

1.5. Youth Perpetrators

Many of the threats that youth experience online are perpetrated by their peers, including sexual solicitation (Wolak et al. 2006) and online harassment (Hinduja and Patchin 2009; McQuade and Sampat 2008; Smith et al. 2008). There is also often an overlap between cyberbullying offenders and victims (Beran and Li 2007; Kowalski and Limber 2007; Ybarra and Mitchell 2004a).

1.6. Adult Perpetrators

Adults who solicit or commit sexual offenses against youth are anything but alike. They are a widely disparate group with few commonalities in psychology and motivations for offending. For instance, child molesters are “a diverse group that cannot be accurately characterized with one-dimensional labels” (Wolak et al. 2008b: 118). Not all child molesters are paedophiles or pedophiles (defined as a strong sexual attraction to prepubescent children); some molesters are not sexually attracted to children, but have other underlying psychological disorders and other factors, such as opportunity, poor impulse control, or a generally antisocial character (Salter 2004). Adults who solicit or molest adolescents are, by definition, not pedophiles (American Psychological Association 2000; World Health Organization 2007), because “[s]exual practices between an adult and an adolescent and sexual aggression against young majors do not fall within the confines of pedophilia” (Arnaldo 2001: 45).

Different terms are used to categorize adult perpetrators. Paedophilia or pedophilia refers to persistent sexual attraction to children; sexual attraction to adolescents is labeled “hebephilia.” In popular discourse, “pedophilia” is typically used to describe those who engage in acts with

any minor, pre- or postpubescent. Attraction is only one of many factors behind why adults engage in sexual acts with minors. Mental disorders including depression and poor impulse control are sometimes factors, as is desire for power, desire to engage in deviant acts, and a mere passing curiosity. It is important to note that many sexual crimes perpetrated against children take place between adults in their twenties and postpubescent adolescents. Little is known about these adult offenders who engage in statutory rape. Consumption of child pornography adds an additional layer of complexity that must be considered, and Section 5.1 provides greater insight into the adult perpetrators who engage in this illegal practice.

The overall prevalence of these offenders in the general population is unknown. Online solicitors of youth, adult offenders participating in Internet-initiated relationships, and consumers of child pornography remain extremely difficult populations to research, as they are mostly anonymous, globally distributed, and may not participate in offline crimes. Similar to many crimes, large-scale quantitative data on offenders—outside of data obtained from those in various stages of incarceration or rehabilitation—does not exist. Collecting meaningful information on these offenders has been challenging and the number of reported offenses might be lower or higher than the actual number of offenders (Sheldon and Howitt 2007: 43). This is a major limitation of survey-based quantitative research, so other methodologies, such as qualitative interviews and focus groups, are referenced where appropriate.

2. Sexual Solicitation and Internet-Initiated Offline Encounters

One of parents' greatest fears concerning online safety is the risk of "predators." This topic is the center of tremendous public discourse and angst (Marwick 2008) and attracts viewers nationwide to the popular TV show *To Catch a Predator*. In 2007, more than half (53%) of adults agreed with the statement that "online predators are a threat to the children in their households" (Center for the Digital Future 2008). Embedded in this fear are concerns about the threats of online sexual solicitation and the possibility that these will lead to dangerous offline encounters between youth and predatory adults.

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 4th–6th graders were asked about their bodies, and 11% of 7th–9th graders and 23% of 10th–12th 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 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; 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). Although 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); chatrooms and instant messaging are still the dominant place where solicitations occur (77%) (Wolak et al. 2006).

A sizeable minority (roughly 10%–16%) of American youth makes connections online that lead to in-person meetings (Berrier 2007; Berson and Berson 2005; Pierce 2006, 2007a; Wolak et al. 2006), but Internet-initiated connections that result in offline contact are typically

friendship-related, nonsexual, and formed between similar-aged youth and known to parents (Wolak et al. 2002). For socially ostracized youth, these online connections may play a critical role in identity and emotional development (Hiller and Harrison 2007).

Fears of predators predate the Internet and were a source of anxiety around children's access to public spaces in the 1980s (Valentine 2004). Although the use of "stranger danger" rhetoric is pervasive, it is not effective at keeping kids safe (McBride 2005). More importantly, 95% of sexual assault cases reported to authorities are committed by family members or known acquaintances (Snyder and Sickmund 2006). In a study of Internet-initiated sex crimes reported to law enforcement, 44% of crimes were committed by family members and 56% were committed by people known to the victim offline, including neighbors, friends' parents, leaders of youth organizations, and teachers; known cases involving strangers are extremely rare (Mitchell et al. 2005b). In other words, the threat of Internet-initiated sex crimes committed by strangers appears to be extremely exaggerated (Finkelhor and Ormrod 2000).

This section outlines what is known about sexual solicitation of minors, those who are perpetrating such acts, and which youth are most at risk.

2.1. Solicitation

An online sexual solicitation is defined as an online communication where "someone on the Internet tried to get [a minor] to talk about sex when they did not want to," an offender asked a minor to "do something sexual they did not want to," or other sexual overtures coming out of online relationships (Finkelhor et al. 2000). This definition encompasses a range of online contact. Though some solicitations are designed to lead to an offline sexual encounter, very few actually do. Some of this contact can be understood as "flirting" (McQuade and Sampat 2008; Smith 2007), and many solicitations are simply meant to be harassing (Biber et al. 2002; Finn 2004; Wolfe and Chiodo 2008).

All told, there are relatively few large-scale quantitative studies concerning the prevalence of online sexual solicitation (Fleming and Rickwood 2004; McQuade and Sampat 2008) and even fewer national U.S.-based studies (Wolak et al. 2006). To date, there has only been one study (N-JOV) that collected law enforcement data on Internet-initiated sex crimes against minors (Wolak et al. 2004), although a follow-up study is nearing completion (J. Wolak, personal communication, September 10, 2008). The first and second Youth and Internet Safety

Survey Surveys (YISS) indicated that 13%–19% of youth have experienced some form of online sexual solicitation in the past year. Given the anonymity of communication, it is often difficult for youth to assess the age of solicitors, but youth reported that they believed that 43% of solicitors were under 18, 30% were between 18 and 25, 9% were over 25, and 18% were completely unknown (Wolak et al. 2006). Despite the prevalence of minor-to-minor sexual solicitation, it remains a particularly under-researched topic.

Online sexual solicitations by adults are of great concern, because some of this type of contact is considered to “groom” youth (Berson 2003) and coerce them to participate in either offline or online sexual encounters. Although conceptually similar to the process that pedophiles use to recruit child victims (Lang and Frenzel 1988), neither online solicitations nor Internet-initiated relationships particularly involve prepubescent children. It is generally assumed that adults use some degree of deception in the grooming process to coerce the youth into sexualized discussions, transmission of self-created images, or offline sexual contact (typically intercourse). In total, 52% of offenders lied about at least one aspect of themselves. Yet significant deception did not appear to be common (Wolak et al. 2008b). A quarter (25%) of adults participating in Internet-initiated sexual relationships with minors shaved off a few years from their real age, a practice also common in online adult–adult interactions (Hancock et al. 2007), and 26% lied about some other aspect of their identity. Only 5% of offenders pretended to be the same age as the youth victim online (Wolak et al. 2004). Wolak, Finkelhor, Mitchell, and Ybarra concluded that, “when deception does occur, it often involves promises of love and romance by offenders whose intentions are primarily sexual” (2008b: 113).

Online solicitations are not generally disturbing to the recipients; most youth (66%–75%) who were solicited were not psychologically harmed by this type of contact (Wolak et al. 2006). A small number of youth (4%) reported *distressing* online sexual solicitations that made them feel “very upset or afraid” (Wolak et al. 2006: 15), or *aggressive* online sexual solicitations (4%), where the offender “asked to meet the youth in person; called them on the telephone; or sent them offline mail, money, or gifts” (Wolak et al. 2006: 15). A small number (2%) of youth reported both aggressive and distressing solicitations. The researchers concluded that although some of the solicitations were problematic, “close to half of the solicitations were relatively mild events that did not appear to be dangerous or frightening” (Wolak et al. 2006: 15). Online

solicitations were concentrated in older adolescents. Youth 14–17 years old reported 79% of aggressive incidents and 74% of distressing incidents (Wolak et al. 2006: 15).

2.2. Offline Contact

The percentage of youth who report Internet-initiated offline encounters in the U.S. ranges from 9%–16% across various locations, sample sizes, administration dates, and wording of surveys (Berrier 2007; Berson and Berson 2005; McQuade and Sampat 2008; Rosen et al. 2008; Wolak et al. 2006). The relative stability and in some cases the decline (Wolak et al. 2006) of the number of Internet-initiated offline meetings involving youth is particularly notable given the rise of adult–adult Internet-initiated offline meetings through dating and personals sites (Bryn and Lenton 2001). Studies in Europe, the United Kingdom, New Zealand, and Singapore show a wider range (8%–26%) of Internet-initiated offline encounters (Berson and Berson 2005; Gennaro and Dutton 2007; Liao et al. 2005; Livingstone and Bober 2004; Livingstone and Haddon 2008), with New Zealand showing the highest prevalence.

The majority of Internet-initiated connections involving youth appear to be friendship-related, nonsexual, and formed between similar-aged youth and known to parents (Wolak et al. 2002). Qualitative studies have shown that Internet-initiated connections are tremendously important for youth who are socially isolated at school and turn to the Internet to find peers who share their interests (Ito et al. 2008). Parents were generally responsible about their children going to real-world meetings resulting from online contact; 73% of parents were aware of real-world meetings and 75% accompanied the minor to the meeting (Wolak et al. 2006). The benign nature of most Internet-initiated meetings can also be inferred from the rarity of those with aggressive or violent overtones, or even those involving sexual contact. Problematic offline sexual encounters resulting from online meetings were found to be extremely rare, and mostly involve older adolescents and younger adults. In one national survey (YISS-2), 0.03% (4 in 1500) of youth reported physical sexual contact with an adult they met online, and all were 17-year-olds who were in relationships with adults in their early twenties (Wolak et al. 2006).

In the small number of offline meetings between minors and adults that involved sex, 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 postpubescent minor having nonforcible sexual relations with an adult, most

frequently in their twenties (Hines and Finkelhor 2007; Wolak et al. 2008b). Of all law enforcement reports of Internet-initiated sexual encounters, 95% of reported cases were nonforcible (Wolak et al. 2004). In one national survey (YISS-1) no instances of Internet-initiated sex were reported, and another (YISS-2), two youth out of 1500 (one 15-year-old girl and one 16-year-old girl) surveyed reported an offline sexual assault resulting from online solicitation. Although identity deception may occur online, it does not appear to play a large role in criminal cases where adult sex offenders have been arrested for sex crimes in which they met victims online; only 5% of youth were deceived by offenders claiming to be teens or lying about their sexual intentions (Wolak et al. 2008b).

Other factors also point to how the minor victims were compliant in the sexual activity. Most (80%) offenders brought up sex in online communication, meaning that “the victims knew they were interacting with adults who were interested in them sexually” (Wolak et al. 2004: 424.e18) before the meeting. Most (73%) of Internet-initiated sexual relationships developed between an adult and a minor involved *multiple* meetings (Wolak et al. 2004), indicating that the minor was aware of the ongoing physical and sexual nature of the relationship. This does not diminish the illegal nature of statutory sex crimes in most states. These are certainly not benign relationships, and some are psychologically harmful to youth (Hines and Finkelhor 2007). At the same time, it is important to recognize the role that some youth—particularly older teens—play in these types of relationships. This is an important policy issue, because “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).

These types of Internet-initiated sexual encounters between an adult and adolescent are also unlikely to be violent. In a nationwide survey of Internet-related contact crimes against youth reported by law enforcement, only 5% of incidents involved violence (such as rape), and none involved “stereotypical kidnappings in the sense of youth being taken against their will for a long distance or held for a considerable period of time” (Wolak et al. 2004: 424.e17). Similarly, despite anecdotal reports (Quayle and Taylor 2001), cyberstalking—a crime where offenders locate youth offline using information found online (Jaishankar et al. 2008)—appears to be very rare (Wolak et al. 2008b).

2.3. Victims

Over the last several years, the focus of research has shifted from offenders to characteristics of adolescents who are solicited online (Peter et al. 2005; Ybarra and Mitchell 2004a; Ybarra et al. 2006). Youth victims of online solicitation tend to be older (McQuade and Sampat 2008), female (Wolak et al. 2006), and experiencing difficulties offline, such as physical or sexual abuse (Mitchell et al. 2007b). Adolescents are more likely to be solicited online, and solicitation of prepubescent children by strangers (including those solicitations leading to an offline sexual encounter) is extremely rare (Wolak et al. 2006). In other words, youth who reported online solicitations tended to be of the age that it is developmentally normal to be curious about sex (Ponton and Judice 2004), and have a troubled home or personal life. Far from being naïve, these adolescents are thought to be more at risk because they “engage in more complex and interactive Internet use. This actually puts them at greater risk than younger, less experienced youths” (Wolak et al. 2008b: 114). This is a perspective that is at odds with studies and programs that have found younger adolescents to be less safety-conscious, and that equate younger age with more risk (Brookshire and Maulhardt 2005; Fleming et al. 2006). However, older youth (teenagers) are more likely to be solicited online and also to respond to these solicitations with real-world encounters, confirmed by both arrests for Internet-initiated sex crimes (Wolak et al. 2004) and youths’ self-reports in surveys (Berson and Berson 2005; McQuade and Sampat 2008; Rosen et al. 2008; Wolak et al. 2006).

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). In qualitative studies, youth who are asked about such encounters draw parallels to spam or peculiar comments from strangers in public settings, noting that ignoring such solicitations typically makes them go away (boyd 2008).

Nearly all (99%) victims of Internet-initiated sex crime arrests in the N-JOV study were aged 13–17, with 76% being high school–aged, 14–17 (Wolak et al. 2007c), and none younger than 12 years old. Youth who reported solicitations in the YISS-2 Study tended to be older as well, with 81% of youth aged 14–17 reporting solicitations (Wolak et al. 2006). The majority (74%–79%) of youth who reported “distressing” or “aggressive” incidents were also mostly aged 14–17 (Wolak et al. 2006).

Girls have been found to receive the majority (70%–75%) of online solicitations (Wolak et al. 2006). Offenders are typically male and tend to solicit females online; in the N-JOV study, 75% of cases involved female victims, and 99% of offenders were male (Wolak et al. 2004). Although there was an overall decline in solicitations, there was also a slight increase in the percentage of males being solicited in YISS-2: 70% of solicited youth were female, and 30% were male (Wolak et al. 2006).

Not all youth are equally at risk. Female adolescents aged 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. 2007b). 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).

2.4. Perpetrators

Although the majority of the public discussion involving sexual contact crimes concerns adult-to-minor solicitation, and the typical image of an online predator is an older male (Wolak et al. 2008b), the reality is that most of the time solicitors are youth or young adults; 43% of the perpetrators of sexual solicitation are known to be other minors, 30% are between 18 and 25, and 18% are of unknown age (Wolak et al. 2006). Though 11% of victims did not know the perpetrator's gender, 73% reported that the perpetrator was male (Wolak et al. 2006). In a small number (14%) of cases, the victim knew the perpetrator prior to the incident (Wolak et al. 2006).

In the N-JOV study, adult offenders who were arrested for Internet-initiated relationships online with minors tended to be male (99%), non-Hispanic white (81%), and communicated with the victim for 1 to 6 months (48%). Offenders were of a wide variety of ages, from 18–25 (23%), 26–39 (41%), and over 40 (35%) years of age (Wolak et al. 2004). However, this study used data from law enforcement, and so does not account for incidents that did not result in an arrest, which is a particularly difficult area to recruit study participants from.

Few studies have explored the dynamics of minor-to-minor solicitation and those who have tend to combine it with broader issues of minor-to-minor harassment, noting that perpetrators of harassment and sexual solicitation tend to have high levels of other psychosocial behavioral issues (Ybarra et al. 2007b). Though online flirting is fairly common among youth

(Lenhart 2007; Schiano et al. 2002) and youth are known to use the Internet as an outlet for sexual thoughts and development (Atwood 2006; Subrahmanyam and Greenfield 2008), little is known about how frequently these interactions are unwanted. Likewise, although many of these encounters are between minors who know each other, little is known about the connection between online sexual talk and unwanted offline sexual encounters (such as “date rape”). This lack of research may be attributed to problems of gaining access to the population, a reluctance to attribute negative psychosocial characteristics to children, reluctance of victims to reveal they were victimized, difficulty in determining the age of the parties, or other methodological difficulties. More research is required to understand the dynamics and complexities of minor-to-minor unwanted sexual solicitation and contact crimes.

3. Online Harassment and Cyberbullying

It is difficult to measure online harassment and cyberbullying because these concepts have no clear and consistent definition. Online harassment or “cyberbullying” has been defined as “an overt, intentional act of aggression towards another person online” (Ybarra and Mitchell 2004a: 1308) or a “willful and repeated harm inflicted through the use of computers, cell phones, and other electronic devices” (Hinduja and Patchin 2009: 5). They may involve direct (such as chat or text messaging), semipublic (such as posting a harassing message on an e-mail list) or public communications (such as creating a website devoted to making fun of the victim). Outside of academic dialogue and discipline, these two terms are frequently used interchangeably, and they have some conceptual similarity (Finkelhor 2008: 26). “Cyberstalking” is another term that captures online activities that may be related to harassment (Jaishankar et al. 2008; McQuade and Sampat 2008), but suffers from a similar lack of conceptual clarity, as definitions of cyberstalking vary widely. Researchers consider it variously as being an attempt to harass or control others online or understand it as an online extension of offline stalking (Adam 2002; Ogilvie 2000; Philips and Morrissey 2004; Sheridan and Grant 2007).

These acts are designed to threaten, embarrass, or humiliate youth (Lenhart 2007). However, cyberbullying frequently lacks characteristics of “schoolyard bullying,” such as aggression, repetition, and an imbalance of power (Wolak et al. 2007a). Some argue that cyberbullying should narrowly mark those acts of harassment that are connected to offline bullying and online harassment should refer to all forms of harassments that take place online, regardless of origin (Wolak et al. 2007a: S51); others argue that online harassment and cyberbullying differ because of the element of repeated behavior in the latter, rather than just one instance (Burgess-Proctor et al. 2009; Hinduja and Patchin 2009). These varying conceptualizations of cyberbullying and Internet harassment likely contribute to the wide range (4%–46%) of youth who report it.

However cyberbullying and online harassment are defined, the reach of cyberbullying is thought to be “magnified” (Lenhart 2007: 5) because the actual location of bullying may be in the school setting (Ybarra et al. 2007a) or away from it. Online bullies use a number of technologies, such as instant-messenger (IM), text and multimedia messaging on a cell phone, e-mail, social network sites, and other websites. Despite this increased reach, cyberbullying is not

reported to occur at higher overall rates than offline bullying. For instance, 67% of teenagers said that bullying happens more offline than online (Lenhart 2007), 54% of grade 7 students were victims of traditional bullying and less than half that number (25%) were victims of cyberbullying (Li 2007b), 42% of cyberbully victims were also school bullying victims (Hinduja and Patchin 2009), and a survey of more than 15,000 students in grades 6–10 found that around 30% were offline bullies or victims (Nansel et al. 2001). In other cases, individuals unknown or anonymous to the victim are the perpetrators of online harassment.

The problem of online harassment of minors is relatively widespread, with 4%–46% of youth reporting being cyberbullied (Agatston et al. 2007; Finkelhor et al. 2000; Hinduja and Patchin 2009; Kowalski and Limber 2007; Kowalski et al. 2007; McQuade and Sampat 2008; Opinion Research Corporation 2006a, 2006b; Patchin and Hinduja 2006; Smith et al. 2008; Williams and Guerra 2007; Wolak et al. 2006), depending on how it is defined; date and location of data collection; and the time frame under investigation. In the United States, 3% of youth aged 10–17 reported three or more cyberbullying episodes in the last year (Ybarra et al. 2006), and 9% of junior high school students said they had been cyberbullied three or more times (Li 2006). A recently published study based on data collected in Spring 2007 found that 17.3% of middle-school youth had been “cyberbullied” in their lifetime, but that nearly 43% had experienced victimizations that could be defined as cyberbullying (Hinduja and Patchin 2009). Relatively few students encounter weekly or daily cyberbullying. In Canada, Beran (2007) found that 34% of Canadian students in grades 7–9 were cyberbullied once or twice, and 19% reported “a few times,” 3% “many times,” and only 0.01% were cyberbullied on a daily basis.

3.1. Victims

About a third of all reports of cyberbullying involve “distressing harassment” (Wolak et al. 2006). Distress stemming from cyberbullying victimization can lead to negative effects similar to offline bullying such as depression, anxiety, and having negative social views of themselves (Hawker and Boulton 2000). As Patchin and Hinduja describe it, “the negative effects inherent in cyberbullying . . . are not slight or trivial and have the potential to inflict serious psychological, emotional, or social harm” (Patchin and Hinduja 2006: 149). Wolak (2006) found that youth (aged 10–17) who were bullied may feel upset (30%), afraid (24%), or embarrassed (22%) and that even the 34% of victims of harassment who were not upset or afraid

may experience effects from bullying, such as staying away from the Internet or one particular part of it, being unable to stop thinking about it, feeling jumpy or irritable, or losing interest in things. Similarly, Patchin and Hinduja (2006) found that 54% of victims were negatively affected in some way, such as feeling frustrated, angry, or sad. This finding is of concern, because negative emotions are often improperly resolved by adolescents through self-destructive behaviors, interpersonal violence, and various forms of delinquency (Borg 1998; Ericson 2001; Rigby 2003; Roland 2002; Seals and Young 2003).

Frequent users of the Internet who talk with strangers online were more likely to report depressive symptoms (Ybarra et al. 2005) and those who are bullies, victims, or both were more likely to report major symptoms (Ybarra and Mitchell 2004a). Depressive symptoms and loneliness are the most common effects of offline bullying (Hawker and Boulton 2000). Other negative school-based effects of online harassment can occur, such as lower grades and absenteeism in school (Beran and Li 2007).

Age-related findings are difficult to compare across studies, as researchers alternately collected age with large ranges (such as “older adolescents”), two-year ranges (such as 12–13 years old), exact age (in years), or grade number (which varies between countries and corresponds only loosely with age). Additionally, some studies focused on a very narrow range of youth, and no conclusions could be drawn on age differences. With these caveats, there appears to be a strong correlation between age and likelihood of victimization. Victimization rates were found to be generally lower in early adolescence (Hinduja and Patchin 2008a; Lenhart 2007; McQuade and Sampat 2008; Ybarra and Mitchell 2004a) and higher in mid-adolescence (around ages 14–15) (Hinduja and Patchin 2008a; Kowalski and Limber 2007; Lenhart 2007; Slonje and Smith 2008). Some studies identified a peak period for online harassment, such as eighth grade (Williams and Guerra 2007) or 15 years of age (Hinduja and Patchin 2008a; Wolak et al. 2006).

Online harassment and offline bullying affect slightly differently aged populations. Reports of online harassment differ slightly from reports of offline bullying declining during middle and high school. The Bureau of Justice Statistics shows a steep decline in offline bullying from seventh to twelfth grades (Devoe et al. 2005), while online harassment tends to peak later, in eighth grade, and declines only slightly (Smith et al. 2008; Wolak et al. 2006). This finding may be due to the fact that only a minority of online harassment is school-related (Beran and Li

2007; Slonje and Smith 2008; Ybarra et al. 2007a) and in some cases has entirely different dynamics than offline bullying. Though school bullying shows a steep decline, online harassment remains level through the end of high school, and has been shown to persist even in college (Finn 2004).

Reports of gender differences are inconclusive, but generally, girls were more likely to be online harassment victims (Agatston et al. 2007; DeHue et al. 2008; Kowalski and Limber 2007; Lenhart 2007; Li 2005, 2006, 2007b; Smith et al. 2008) and more likely to be distressed by being harassed (Wolak et al. 2007a). Girls are more at risk for online harassment, whereas boys are typically more likely to be physically bullied offline (Devoe et al. 2005). It bears mentioning that the some studies found no difference in gender with respect to percentages of victims of online harassment (Hinduja and Patchin 2008a), although there are clear qualitative differences across gender in the actual *experience* of being cyberbullied (Burgess-Proctor et al. 2009) and in their emotional response to victimization (Burgess-Proctor et al. 2009; Hinduja and Patchin 2009).

3.2. Perpetrators

Youth are most often involved with bullying other youth online. 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 age 18 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). Between 11%–33% of minors admit to harassing others online (Kowalski and Limber 2007; McQuade and Sampat 2008; Patchin and Hinduja 2006; Wolak et al. 2006). Consistent with offline bullying, online harassers are typically the same age as their victims (Kowalski and Limber 2007; Slonje and Smith 2008; Wolak et al. 2006, 2007a) and half of victims reported that cyberbullies were in their same grade (Stys 2004).

In online contexts, perpetrators may 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. Between 37%–54% of bullied minors report not knowing the identity of the perpetrator or perpetrators (DeHue et al. 2008; Kowalski and Limber 2007; Li 2005, 2007a; Wolak et al. 2007a). Wolak et al. (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.

Mid-adolescents were more likely to be perpetrators (Smith et al. 2008; Williams and Guerra 2007) and age (ranging from 13–18) was correlated with likelihood to engage in online harassment (Raskauskas and Stoltz 2007). Boys were identified as more likely to be online harassers (DeHue et al. 2008; Li 2007a; Williams and Guerra 2007), yet these findings that online harassers are primarily male against conflict with other research showing that females may increasingly harass online because the forms of harassment common online (shunning, embarrassment, relational aggression, social sabotage) are more similar to their own modes of offline bullying (Ponsford 2007). Some studies did find girls to be more prone to certain types of harassment behavior, such as the spreading of rumors (Lenhart 2007) and being distressed by harassment (Wolak et al. 2006), yet others found no gender difference in perpetrators (Hinduja and Patchin 2008a; Li 2006; Wolak et al. 2007a; Ybarra and Mitchell 2004b). Such conflicting results suggest a need for different methodological approaches and measures of harassment that capture the variety of ways bullying can be perpetrated online by both males and females.

3.3. Overlaps in Victimization and Perpetration

Distinguishing between victims and perpetrators can be challenging, because some victims of online harassment may themselves be perpetrators. Though this issue is not well studied, between 3%–12% of youth have been found to be both online harassers and victims of online harassment (Beran and Li 2007; Kowalski and Limber 2007; Ybarra and Mitchell 2004a). Due to methodology issues and anonymity, the rate of overlap is likely much higher. Aggressor–victims experience combinations of risks and are “especially likely to also reveal serious psychosocial challenges, including problem behavior, substance use, depressive symptomatology, and low school commitment” (Ybarra and Mitchell 2004a: 1314). The overlap between online perpetrators and victims shares conceptual similarities to offline “bully–victims” (those who are both bully and are the victims of bullies), a concept reported to include between 6%–15% of U.S. youth (Haynie et al. 2001; Nansel et al. 2001). Although these studies conceive of the victim–perpetrator overlap as being related to individual psychosocial qualities, the relationship may also be directly related. The affordances of Internet technology may allow both online and offline victims to retaliate to harassment. In a recent study, 27% of teenaged girls

were found to “cyberbully back” in retaliation for being bullied online (Burgess-Proctor et al. 2009).

Too little is known about the relationship between online bullies and victims, reciprocal bullying, and cross-medium shifts between bullies and victims. This area requires further examination.

3.4. Offline Connections

Studies differ on whether 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. With cyberbullying, bully and victim populations overlap but sometimes involve entirely unknown harassers. The most frequent and simple way to measure offline bullying is whether it was experienced in a school setting (although exact location is difficult to pinpoint, given the various technologies and locations involved). By this measure, less than half of online harassment is related to school bullying, either through location (occurring at school) or peers (offender or target is a fellow student). Ybarra found that 36% of online harassment victims were bullied at school (Ybarra et al. 2007a), and 56% of Canadian students in grades 7–9 who were bullied at school were also victims online (Beran and Li 2007). In other studies, over half of known bullies (or around 25% of the total number of cyberbullies) were identified as being from school, showing some overlap with school environments (Slonje and Smith 2008). Other studies show connections between online and offline bully perpetration (Raskauskas and Stoltz 2007) and online and offline bully victimization (Beran and Li 2007; Kowalski and Limber 2007; Slonje and Smith 2008: 152; Ybarra et al. 2007a). Although many studies have not examined whether the perpetrators and victims online are the same as offline, there appears to be a partial overlap, possibly stemming from the very broad definition of the activity. For example, Hinduja and Patchin (2007) found that 42% of victims of cyberbullying were also victims of offline bullying, and that 52% of cyberbullies were also offline bullies.

The overlap between offline bullying and online harassment also varies depending on who is reporting the relationship. For instance, 29% of online perpetrators reported harassing a fellow student, while 49% of online victims reported being harassed by a fellow student (Kowalski and Limber 2007). Those who are engaged in online harassment but not offline

bullying may see the Internet as a “place to assert dominance over others as compensation for being bullied in person” or “a place where they take on a persona that is more aggressive than their in-person personality” (Ybarra and Mitchell 2004a). Some victims do not know who is bullying them (Ybarra and Mitchell 2004a), although many do (Hinduja and Patchin 2009).

Wherever harassment takes place, the effects can have an impact on school. For example, those bullied outside of school were four times more likely to carry a weapon to school (Nansel et al. 2003). Moreover, Hinduja and Patchin (2007) found that youth who experience cyberbullying are more likely to report participating in problem behaviors offline (as measured by a scale including alcohol and drug use, cheating at school, truancy, assaulting others, damaging property, and carrying a weapon).

3.5. Connections to Solicitation

The scant research that has been performed on the connections between online harassment and solicitation indicate that there is a minority overlap between the two, both as victims and perpetrators (Ybarra et al. 2007b). Youth who are “perpetrator–victims” (both perpetrators and victims of Internet harassment and unwanted sexual solicitation) constitute a very small minority of youth, but they reported extremely high responses for offline perpetration of aggression (100%), offline victimization (100%), drug use such as inhalants (78%), and number of delinquent peers (on average, 3.2). This group was also particularly likely to be more aggressive offline, be victimized offline, spend time with delinquent peers, and have a history of substance abuse.

4. 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 pornographic content that is legal for adults to consume. Other problematic content that emerges in research includes hate speech and content discussing or depicting self-harm. 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. This literature review focuses on the first two issues. The third includes ongoing debates over the behavioral and psychological effects of immersive transmedia exposure to this type of content (de Zengotita 2006; Glassner 1999; Jenkins 2006) that are outside the scope of this review.

4.1. Pornography

Encounters with pornography are not universal, but they are common. 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). These numbers represent an increase from 2000 (Mitchell et al. 2007a). Minors saw pornography through either wanted (deliberate) exposure, unwanted (accidental) exposure, or both (Cameron et al. 2005; Flood 2007; Greenfield 2004; McQuade and Sampat 2008; Mitchell et al. 2003; Peter and Valkenburg 2006; Sabina et al. 2008; Wolak et al. 2007b; Ybarra and Mitchell 2005). Exact statistics on how pervasive pornographic content is on the Internet has been heavily disputed (Hoffman and Novak 1995; Rimm 1995; Thomas 1996), but it does not appear to be as pervasive as initially thought (Mehta 2001; Mehta and Plaza 1997).

Wanted exposure to pornographic material includes inputting sexual terms into a search engine, downloading adult media, and otherwise seeking out a sexually themed website (such as typing a known adult URL into a web browser). One case study suggested that most unwanted

exposure comes from “spam” emails, mistyping of URLs into a web browser, and keyword searches that “produce unexpected results” (White et al. 2008). In YISS-2, 34% of youth reported either only wanted exposure or both unwanted and wanted exposure (Wolak et al. 2006). Wanted exposure is also indicated by 19%–21% of minors who deliberately visited a pornographic website (Wolak et al. 2006). In a 1999 study, 21% of seventh through tenth graders were found to visit such a site for more than three minutes in the past month (Stahl and Fritz 1999), and in YISS-1 and YISS-2, 19%–21% of youth admitted deliberately going to an “X-rated” website (Wolak et al. 2006). Youth visit these sites for a variety of reasons, such as for sexual excitement, curiosity, or for informational purposes (Sabina et al. 2008).

Unwanted exposure is a new concern online, because “before development of the Internet, there were few places youth frequented where they might encounter unsought pornography regularly” (Wolak et al. 2007b: 248). In YISS-1, 25% of minors aged 10–17 viewed unwanted pornography in the past year. About 6% of this group reported being “very or extremely upset” by unwanted exposure to online pornography (Mitchell et al. 2003). These figures increased in 2005 when YISS-2 was administered and 34% of minors aged 10–17 reported being exposed to unwanted pornography, and 9% of them 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. 2007b).

Rates of exposure vary in other countries, and in some cases were reported to be higher than in the United States (Flood 2007; Hasebrink et al. 2008; Livingstone and Bober 2004; Lo and Wei 2005). In addition to the previously mentioned sources of methodological variance, increased overseas rates could be due to increased acceptance of sexualized topics, fewer technical measures such as blocking sites, and varying cultural and home environments. For instance, in a survey of 745 Dutch teens aged 13–18, 71% of males and 40% of females reported exposure to adult material in the last 6 months (Peter and Valkenburg 2006), a far higher number than in similar U.S.-based studies.

Older teens are more likely to encounter pornographic material through searching or seeking. When asked about their preadult exposure, the majority in a study of 563 college undergraduates reported seeing Internet pornography between ages 14–17, and only a very small percentage of boys (3.5%) and girls (1.5%) reported exposure before age 12 (Sabina et al. 2008).

Although the Internet plays a dominant role in adult fears and older youth are more likely to encounter pornographic content online, younger youth are more likely to encounter offline adult material such as movies or magazines than Internet-based pornography. Pardun (2005) found that of seventh and eighth graders who are exposed to nudity, more are exposed through TV (63%) and movies (46%) than on the Internet (35%). Ybarra and Mitchell found that 4.5% of younger Internet users reported both online and offline exposure, 3.6% reported online-only, and 7.2% report offline-only exposure in the past year; they concluded that, “concerns about a large group of young children exposing themselves to pornography on the Internet may be overstated” (2005: 473).

Most studies found that males are more frequently exposed to pornographic material than females (Cameron et al. 2005; Flood 2007; Lenhart et al. 2001; Nosko et al. 2007; Peter and Valkenburg 2006; Sabina et al. 2008; Stahl and Fritz 1999; Wolak et al. 2007b; Ybarra and Mitchell 2005). In some cases, gender differences were quite pronounced between types of exposure; 2% of Australian girls reported wanted exposure, while 60% reported unwanted exposure (Flood 2007), and males were more likely to seek out a wider variety of pornography and more extreme content (Sabina et al. 2008). Despite the wealth of evidence that girls are at greater risk of unwanted exposure, most studies have focused on males who are seen as more likely to seek out content. Youth often (44%) sought out this content “with friends or other kids” (Wolak et al. 2006). The dynamics of small groups of youth, particularly with young males, may lead to transgressive behavior such as viewing of adult content; wanted exposure was higher for minors who were teenagers, male, used the Internet at friends’ houses, and were prone to breaking rules (Wolak et al. 2007b).

4.2. Violent Content

Violent content on the Internet can take the form of movies and images, as well as video games (Thompson and Haninger 2001), many of which are networked (Lenhart et al. 2008). Nearly half (46%) of parents say they are “very concerned” about the amount of violent content their children encounter (Rideout 2007). In the UK, nearly one-third (31%) of youth reported having ever seeing “violent or gruesome material online” (Livingstone and Bober 2004), as did 32% of online teenagers in Europe, in a meta-analysis (Hasebrink et al. 2008).

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 video games, on news sites, and through videos that are circulated among youth.

Video games are a common genre of media in which youth encounter violent content. Nearly all minors (94%) have played some form of video game, and nearly half (49%) of underage game players reported playing at least one M (mature)-rated title in the previous six months (Olson et al. 2007). Although gaming is viewed as a male activity, data suggests that 40% of game players and 44% of online game players were female (Entertainment Software Association 2008). Boys tend to prefer different types of games than do girls, and gender differences exist in how they deliberately participate (“wanted” exposure) in violent video games. Young boys tend to play more violent video games (Griffiths et al. 2004; Gross 2004; Olson et al. 2007), and girls tend to prefer games that include social interaction, nonviolent content, and fewer competitive elements (Hartmann and Klimmt 2006).

We believe that some degree of production by minors of violent content is likely, but no studies have specifically looked in depth at minors viewing or creating violent movies online, probably due to the relatively early stage of the adoption of video sites.

4.3. Other Problematic Content

Hate speech and content involving self-harm are two understudied areas that raise concern in terms of youth exposure. Although exposure to hate speech and self-harm websites are not commonly discussed in public discourse, this content presents an additional layer of concern.

Hate speech is a specific type of online content that is designed to threaten certain groups publicly and act as propaganda for offline organizations. These hate groups use websites to recruit new converts, link to similar sites, and advocate violence (Gerstenfeld et al. 2003), as well as threaten others (McKenna and Bargh 2000). An analysis of U.S.-based extremist groups found that these types of sites predominantly were used for sharing ideology, propaganda, and recruitment and training (Zhou et al. 2005).

Viewers generally find these types of websites threatening (Leets 2001) and adolescents are believed to be more likely to be persuaded by these biased and harmful messages (Lee and

Leets 2002). There is also concern that a small number of youth converts may conduct either offline or online (“cyberhate”) crimes or engage in online harassment (Deirmenjian 2000). These groups are quite technology-savvy, and have adopted new technologies popular with youth, such as blogs (Chau and Xu 2007).

Though online hate groups appear to use the Internet as a way to spread their messages and promote threatening content, the number of such sites is still miniscule in comparison to the total sites in existence. Although it is difficult to attain an accurate tally of these types of sites, according to the Southern Poverty Law Center, there were 497 hate sites in 2003 (Southern Poverty Law Center 2004). How frequently youth encounter hate speech and other such content on a national scale is unknown, but is not limited to websites. In a limited, small-scale analysis of chat transcripts, chat participants had a 19% chance of exposure to negative racial or ethnic remarks in monitored chat and a 59% chance in unmonitored chat (Tynes et al. 2004). Also, mere exposure is not the biggest problem: “Recent news articles and studies have shown that children and adolescents are increasingly involved in online hate speech” (Tynes et al. 2004: 267). Similar to the shift of discussion in cyberbullying and solicitation to examine the role of minors who produce content, we must be aware of the possibility that minors are not just consumers, but active producers and propagators of racist, anti-Semitic, and sexist information online.

Self-harm-related websites introduce another element of problematic content. There is tremendous public concern that sites dedicated to enabling self-injury and suicide or those that encourage anorexic and bulimic lifestyles (otherwise known as “pro-ana” and “pro-mia” sites) encourage youth to engage in problematic activities (Shade 2003), particularly given the addictive nature of some of these practices (Whitlock et al. 2006). Many sites concerning self-harm are structured as support groups and can actually benefit youth and enable them to get help (Murray and Fox 2006; Whitlock et al. 2006), but the act of identifying such behaviors with disorder may actually impede recovery (Keski-Rahkonen and Tozzi 2005).

At this point, very little is known about teens that participate in self-harm websites and even less about the interplay between participation in the websites and participation in self-harm. What is known is that youth engaged in deliberate acts of self-harm are much more likely to be contending with other psychosocial issues, have a history of physical or mental abuse, and have a high degree of parent–child conflict (Mitchell and Ybarra 2007). Likewise, those who are

engaged in deliberate acts of self-harm are much more likely to engage in other risky online behaviors (Mitchell and Ybarra 2007). Efforts to banish and regulate this content have pushed it underground, creating the rise of eating disorder communities like those labeled “pro-ana” and “pro-mia” that discuss their practices without ever mentioning anorexia or bulimia.

5. Child Pornography

“Child pornography” consists of images and videos that depict minors (under the age of 18 in the United States) in suggestive poses or explicit sex acts. Though some content involving children in suggestive poses is not illegal, child pornography is illegal in the United States (Jenkins 2001: 3). Child pornography is a particularly horrific crime, because it involves pictures and movies that are a record of a “sexual assault on a child” (Taylor and Quayle 2003). Child pornography may not directly physically harm youth each time it is viewed by an adult; however, child pornography perpetuates the idea that sexual relations with children by adults are acceptable. Those who view child pornography, for instance, may erroneously believe that the children involved are voluntary participants who enjoy the act, failing to recognize a power differential (Howitt and Sheldon 2007).

The COPINE project in Europe found that child pornography offenders frequently collect and organize illegal content that depict child molestation (Taylor and Quayle 2003), as did similar studies in the United States (Wolak et al. 2005). The idea of this content being used in the fantasies of child sex offenders (Sheldon and Howitt 2007) is disturbing to both victims and the public at large. Although child imagery is present online that is legal and merely erotic (such as children shown partly nude in normal situations), most of the studies below concern graphic images of sex acts involving youth. Jenkins (2003) estimates a core worldwide population of 50,000 to 100,000 users of online child pornography, excluding casual browsers, although this number is difficult to verify (Sheldon and Howitt 2007).

In addition to being a crime in and of itself, child pornography also factors into sexual solicitation. Some offenders expose youth to child pornography during the grooming process and make videos and images of offline sexual acts with youth, or ask youth to take sexual pictures of themselves. Once these videos and images are uploaded, it is nearly impossible to keep them from being traded, downloaded, and viewed by third parties. Taylor and Quayle describe the way this content can never be deleted as, “a permanent record of crime, and serves to perpetuate the images and memory of that abuse” (Taylor and Quayle 2003: 24).

5.1. Child Pornography Offenders

Adults who view child pornography online are likely to be pedophiles (Seto et al. 2006), although not all are. Some adults who are not pedophiles may have a passing and casual interest in, or arousal by, sexualized media involving children (Briere and Runtz 1989; Hall et al. 1995; Malamuth and Check 1981). “Child pornography” on the Internet does not exclusively feature prepubescent children—many images online are of adolescent minors (Taylor and Quayle 2003). A number of child pornography offenders are true pedophiles that use the Internet to satisfy their attraction to prepubescent youth by locating and collecting images and movies featuring child nudity or sex acts (Frei et al. 2005; Sheldon and Howitt 2007; Wolak et al. 2004). Still other offenders who are for the most part not active on the Internet produce videos and images of child molestation or statutory rape, which they distribute in a variety of ways, and which may eventually end up online (Wolak et al. 2005). Some child pornography offenders feel a need to obsessively collect and catalog a range of sexually deviant material, not limited to images and movies featuring children (Quayle and Taylor 2002, 2003). Though it is important to understand how exposure to media (such as child pornography) leads to cognitive change amongst offenders and examine the intrinsic motivation for these offenses, understanding the primary motivation of offenders (even for horrific crimes) is outside the scope of this review.

There is no typical Internet sex offender, and “mixed offenders” (who both view or create child pornography and molest children) in particular vary greatly in motivation. Some are sexually attracted to children, others collect extreme pornography of many varieties, and others are offline molesters who upload images of the abuse to the Internet.

5.2. Child Pornography and Sexual Solicitation

Some claim a direct relationship between consumption of child pornography and contact offenses (Kim 2005)—particularly the media (Potter and Potter 2001)—but the research that has been performed on the topic in focus groups, interviews, and historical analyses on incarcerated or rehabilitating offenders found that between 4%–41% of contact offenders possessed child pornography (Frei et al. 2005; Fulda 2002, 2007a, 2007b; Mitchell et al. 2005a; Seto et al. 2006; Sheldon and Howitt 2007; Webb et al. 2007). Much of this variance may be explained by the varying methodologies and subjects under study; some investigate the issue by researching child

pornography offenders using qualitative interviews, others have examined arrest statistics of contact offenders.

Several researchers have concluded that few child pornography offenders are also online or offline contact offenders. Sheldon and Howitt concluded that “many of the offenders we studied did not seem to stray beyond the Internet for their paedophilic activities” (Sheldon and Howitt 2007: 120). Mitchell, Finkelhor, and Wolak wrote that, “despite its plausibility from anecdotal accounts, there is little research confirming a regular or causal role for pornography in child molestation” (Mitchell et al. 2003: 334). Bensimon (2007) noted that the mixed results of studies on the role of pornography on offending (not limited to child pornography or child offenses) resist conclusions.

The connection between child pornography and molestation is still much disputed, and we make no attempt to reconcile the various worthy theoretical stances on this important issue. A typology of child pornography and offenders is simply outside of the scope of this report. What is certain is that the activities of “mixed offenders” intersect with youth safety in several critical ways. Sheldon and Howitt (2007) argue that there are three primary reasons to be concerned about online child pornography: offenders who view and trade child pornography create a demand, “deviant sexual fantasies based on Internet images may fuel a need to sexually abuse other children,” and child pornography is sometimes created during the grooming process by both solicitors and youth victims (which may or may not be initiated online). Similar to how child pornography viewers were widely varied in their motivations, “there was no typical scenario for [child pornography] production” (Wolak et al. 2005: 44). The N-JOV study found that 21% of Internet-initiated sex crimes involved the victim being photographed in a “suggestive or sexual pose,” 9% of offenders sent the victim adult pornography, and 10% of offenders sent the victim child pornography (Wolak et al. 2004). Additionally, some offenders may send pornographic images of themselves (such as genitals) to potential victims, or request them from potential victims. Youth victims of Internet solicitations said that the offender requested a sexual picture from them or sent them a sexual photograph (such as of their genitals) 15% of the time (Wolak et al. 2006). One in five online child molesters took “sexually suggestive or explicit photographs of victims or convinced victims to take such photographs of themselves or friends” (Wolak et al. 2008b: 120). Compared with the collection habits of child pornography collectors, requests for minors to self-produce pornography more directly affects

online youth. Despite low rates of compliance among youth, this is a serious issue for both contact and child pornography offenses, as, “[even] if only a small percentage cooperate, considering such requests flattering, glamorous, adventuresome, or testament of their love and devotion, this could be a major contribution to the production of illegal material” (Mitchell et al. 2007b: 201).

Adults are not exclusively involved in the production of sexual content depicting youth. An additional issue that intersects this topic is the presence of youth-generated sexual photographs intended for viewing by other minors. Though not intended for adult consumption, the Internet may play a role in spreading such camera phone, webcam, and digital camera photos, potentially putting them within reach of child pornography consumers. One of the first surveys to include questions on the topic, on a large number of students in New York, found that 3% of seventh through ninth graders asked for “naked pictures from another Internet user” (McQuade and Sampat 2008), showing that a small number of minors request self-produced erotic material.

6. Risk Factors

With all three types of threats (sexual solicitation, online harassment, and problematic content), some youth 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. 2007, 2007b).

6.1. Online Contact with Strangers

Chatting with strangers online is a common activity, and between 45% and 79% of U.S. youth participate in this activity (McQuade and Sampat 2008; Stahl and Fritz 1999; Wolak et al. 2006). 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). Recent research also suggests that talking to strangers may not be innately risky; those involved in other risky behaviors (such as making rude or nasty comments, using file-sharing software to download images, visiting X-rated web sites, or talking about sex to people online) in addition to chat are more likely to receive aggressive solicitations (Wolak et al. 2008a; Ybarra et al. 2007). 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?

As with any type of correlation, these combinations of risk factors are not causally linked, and it is impossible to currently assess cause and effect. There is no consensus on whether youth are more at risk because they talk to strangers or at-risk youth are more likely to talk to strangers; various studies identify both parties are partly to blame for how these sexual relationships develop. Youth routinely lie when presenting themselves online, a small number request erotic material of other minors, minors who are solicited have a host of sociopsychological factors, and “online solicitation” is not exclusively meant to entice victims into sexual relationships. That

said, there is a widespread public belief, which is backed up by some research, that adult solicitors coerce, or “groom,” youth into sexualized situations, and certain social media and technologies mediate risk differently.

Making connections online that lead to offline contact are not inherently dangerous. A regional study in New York found that 10% of seventh and eighth graders and 14% of tenth through twelfth graders have invited online friends to meet offline (McQuade and Sampat 2008), but Internet-initiated connections that result in offline contact are typically friendship-related, nonsexual, and formed between similar-aged youth and known to parents (Wolak et al. 2002). For socially ostracized youth, these online connections may play a critical role in identity and emotional development (Hiller and Harrison 2007).

6.2. Posting of Personal Information

Youth frequently post information of all sorts (text, images, video) online through social media such as social network sites (SNSs). Though investigation in this area is quite new, it appears that only a small number of teens are posting the most sensitive contact information such as a phone number on a public profile (Lenhart and Madden 2007). Jones et al. concluded that “the inclusion of offline contact information was an anomaly in user profiles” (Jones et al. 2008), but nearly two-thirds of members posted more innocuous media such as a picture. Pierce (2007b) found a majority of youth on MySpace posted information such as a picture (81%), hometown (93%), and first name (53%). Only a small minority (5%–11%) of youth posts more sensitive information, such as a first and last name or phone number (Lenhart and Madden 2007; Pierce 2007b). Analysis by Hinduja & Patchin (2008b) of approximately 1,500 randomly retrieved MySpace profiles revealed only a minority of members provided descriptive information such as full name (9%) or phone number (0.3%), while a majority posted a picture (57%) and many (27.8%) included the name of their school. Interestingly, a follow-up study by the same authors found a significant increase in the percentage of youth posting their full name and a significant decrease with one’s school (Burgess-Proctor et al. 2009), pointing to somewhat unpredictable trends in the way youth are disclosing information on their SNS. Youth may disclose information differently; males were found to post personal information, and females posted images (Ybarra et al. 2005). More males were also found to have public profiles, and females were more likely to have private profiles (Burgess-Proctor et al. 2009).

Posting personal or identifying information is often viewed as a risky behavior, although research suggests that the mere act of posting information may not in itself be a risk factor. In explaining why there is no correlation, Wolak, Finkelhor, Mitchell, and Ybarra note that because posting information is common on these very popular sites, “in general, behaviors manifested by large numbers of people fail to predict events that are relatively uncommon” (Wolak et al. 2008b: 117). Rather risk is associated with interactive behavior. Other risky habits may be better predictors, and more related to why youth are at risk. In other words, the same psychosocial factors that place youth at risk for online solicitation and bullying outweigh the risk of posting personal information online. For instance, “talking with people known only online (‘strangers’) under some conditions is related to interpersonal victimization, but sharing of personal information is not” (Ybarra et al. 2007: 138).

These recent findings are contrary to many suggested best practices publicized by groups devoted to the protection of youth online. Despite these efforts, the number of youth revealing personal information increased from 2000 (11%) to 2005 (35%) (Wolak et al. 2006). During this time of rapid technological change and transition, it remains to be seen how the risk of transmission of personal information interacts with or mediates other risk factors. In YISS-2, researchers concluded that, “it is not clear what kinds of information are particularly problematic, or exactly what the risks are with respect to the different situations in which youth disclose personal information online” (Wolak et al. 2006: 50).

One area of concern involves youth who engage in age deception, indicating that they are older than they are (Gross 2004; McQuade and Sampat 2008). This may lead young adults to believe that they are interacting with someone who is of age when they are not. Little is currently known about the intersection of this risk behavior and sexual victimization.

As our knowledge of the area expands, we can likely draw more meaningful conclusions about how and where it is appropriate to reveal personal information.

6.3. Sharing of Passwords

By sharing their passwords with friends and peers, youth run the risk of being impersonated online and having their accounts used in acts of harassment. Little is known about how often youth share their passwords or in what circumstances. Pew Internet research from 2001 found that 22% of youth aged 12–17 had shared a password with a friend or someone they

know (Lenhart et al. 2001). More recently, McQuade and Sampat (2008) found that 13% of fourth through sixth graders and 15% of seventh through ninth graders in upstate New York experienced someone using their password without their permission and a slightly smaller percentage of youth had someone else impersonate them online. In a qualitative study on teenagers and social media, boyd (2008) found that teens frequently share their passwords with friends and significant others, both as a symbol of trust and in order to get technical help. When the friendship falters, teens sometimes use this privileged access against one another. It is likely this password sharing introduces a risk with respect to online harassment, but little is currently known about this practice.

6.4. Depression, Abuse, and Substances

Depression, physical abuse, and substance abuse are all strongly correlated with various risky behaviors that lead to poor choices with respect to online activities. Depressed youth were more likely to report increased unwanted exposure to online pornography (Wolak et al. 2007b), online harassment (Mitchell et al. 2007a; Ybarra 2004; Ybarra et al. 2004), and solicitation (Mitchell et al. 2007a). Risk for online harassment was particularly pronounced among depressed male youth, who were eight times more likely to be victimized than nondepressed male youth (Ybarra 2004). Suicidal ideation has also been significantly correlated with online harassment victimization among adolescents (Hinduja and Patchin 2009). Self-harm, often a physical manifestation of depression, is also correlated with other risky behaviors that increase the likelihood of risk (Mitchell and Ybarra 2007, 2007; Mitchell et al. 2005a). Depressed youths were also prone to a host of other risk factors, and were more likely to be heavy Internet users and talk with strangers online (Ybarra et al. 2005), making it difficult to untangle where the risk lies.

Minors who formed close relationships online were more likely to be a victim of physical or sexual assault, and have at least one negative life event (Wolak et al. 2003a). Likelihood of solicitation and harassment has been correlated with offline sexual and physical abuse (Mitchell et al. 2007a, 2007b).

Online harassers were found to be three times more likely to be frequent substance users (Ybarra and Mitchell 2004b). Likewise, victims of solicitation were twice as likely to report substance use (Mitchell et al. 2007a). Youth who were both perpetrator–victims of Internet

harassment and unwanted online sexual solicitation were the heaviest users (Ybarra et al. 2007b). This finding parallels offline settings, where bullies tend to have used alcohol or other substances (Ybarra and Mitchell 2007). Substance abuse also appears to be linked to other risky behaviors. For instance, ninth-grade students who chatted online were more likely to drink or do drugs in the last year (Beebe et al. 2004).

6.5. Poor Home Environment

A poor home environment full of conflict and poor parent–child relationships is correlated with a host of online risks (Wolak et al. 2003a; Ybarra and Mitchell 2004b). Home is where nearly all (91%) of youth reported using the Internet (Wolak et al. 2006) and by 2007 the majority (75%) of homes had broadband access (Center for the Digital Future 2008). A poor home environment full of conflict and poor parent–child relationships is correlated with a host of online risks. High parental conflict was correlated with higher online sexual victimization (Wolak et al. 2003a) and a poor caregiver–child relationship (with poor emotional bonds, infrequent discipline, and infrequent monitoring) was related to increased online harassment (Ybarra and Mitchell 2004b). These data mirror findings in the real world, where low parental monitoring is correlated with a host of negative consequences, such as increased likelihood of violence over time (Brendgen et al. 2001), police contact (Pettit et al. 2001), and traditional bullying (Patterson and Fisher 2002; Steinberg and Silk 2002), while a *positive* parental relationship mediated effects of poverty and other demographic indicators (Barnow et al. 2001).

Greenfield wrote that, “a warm and communicative parent–child relationship is the most important nontechnical means that parents can use to deal with the challenges of the sexualized media environment” (Greenfield 2004: 741). The vast majority of parents (90%) are concerned about their child’s online safety (Wolak et al. 2006), and about half have discussed related topics (such as online sexualized talk, adult pictures, and harassment) with their children. About a third received this information from school. These instructions appear to be helpful, although the positive benefits may relate more to a healthy home life. Those parents who talked with their children about Internet safety or had rules for using the Internet generally had a better environment for most types of Internet threats., and parenting style was related to the techniques used to restrict access of minors to the Internet (Eastin et al. 2006).

A positive home environment inoculates youth against a host of dangers. Parents who talked about Internet dangers had more safety-conscious children (Fleming et al. 2006). More family rules regarding the Internet were correlated with less risk of a face-to-face meeting with someone met online (Liau et al. 2005). Family cohesion and shared activities led to less exposure to negative content such as pornography (Cho and Cheon 2005).

Despite an interest in the topic, parents generally believed that online issues of harassment, solicitation, and access to adult content were less prevalent than they actually were. Parents in the United States believed online harassment to be less prevalent than data showed (DeHue et al. 2008), and 33% of youths aged 9–19 in the UK reported online harassment, while only 4% of parents believed their children encounter online harassment (Livingstone and Bober 2004). Similarly, parents also underestimated the amount of adult content youth were exposed to either accidentally or deliberately (Cho and Cheon 2005) and the amount of information adolescents posted online (Rosen et al. 2008). These findings echo similar earlier studies that showed adults weren't savvy to the latest developments online; in 2002 parents were found to underestimate how frequently their children engage in activities such as e-mail (17% compared with 45%), posting online personals (68% compared with 81%), and corresponding with strangers (30% compared with over 50%) (Computer Science and Telecommunications Board National Research Council 2002: 165).

The underestimation of incidents may be due to the very infrequent reporting of incidents by youth to parents or other adults. Only around a third of those harassed reported the occurrence to a parent or guardian (DeHue et al. 2008; Opinion Research Corporation 2006b; Patchin and Hinduja 2006; Wolak et al. 2006) and less frequently told another adult such as a teacher. Wolak, Mitchell, and Finkelhor (2006) found that 63% did not report the incident because they thought it was “not serious enough.”

6.6. Intensity of Online Participation

Though 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), but as these tools are broadly popular, this does not make them unique. One interesting note in this data is that youth who are not solicited are much

more likely to indicate that gaming is one of their top Internet uses as compared to those who are solicited (Ybarra and Mitchell 2008).

7. Genres of Social Media

Many of the studies focus on the Internet at large, yet youth face different risks in different online environments. Sometimes this risk is because technologies facilitate certain communication between adults and minors or among minors. For instance, on SNSs, 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 are another factor at play. In some types of environments, such as gaming communities, it is more normative for youth to interact with people they don't know. At-risk youth are more attracted to some environments, elevating their levels of risk, as is demonstrated when depressed or sexually promiscuous youth are heavier users of online chat. Finally, certain environments provide means to actively combat solicitation and harassment, such as by blocking or ignoring users.

In understanding the interplay between genres of social media and threats to minors, it is also important to note that different media play a different role at different times because of trends and fads. Thus, comparing data across years is often difficult because youth adoption of particular genres of social media has changed rapidly over the years.

The risks presented by the newest genre of social media—social network sites—with respect to solicitation, and to a lesser degree with harassment, appear to be consistent with Internet risks more broadly and lower than those in other media (Ybarra and Mitchell 2008). 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.

7.1. Chatrooms and Instant Messaging

Chatrooms and instant messaging have been the most prevalent media in online solicitation, as well as more general “cybersex” activities (Lamb 1998) and harassment of minors. The current literature suggests that, “the nature of chat rooms and the kinds of interactions that occur in them create additional risk” (Wolak et al. 2007c: 329). For example, synchronous media that enables ongoing conversations may be important for grooming youth and coercing them into nonforcible relationships. On average, half of youth who report

harassment identified that it first occurred in chat rooms or through instant messaging (Kowalski and Limber 2007; Opinion Research Corporation 2006a, 2006b; Wolak et al. 2006).

Those soliciting youth online even more frequently use chat rooms and instant messaging. These technologies account for between 77%–86% of solicitation attempts and Internet-instigated relationships leading to offline sexual encounters; authorities reported that in more than 86% of Internet solicitation incidents resulting in arrest, youth were first contacted over chat (76%) or instant messaging (10%) (Wolak et al. 2004). Similarly, from the perspective of potential victims, 77% of youth reported being solicited through chat (37%) or instant messaging (40%) (Wolak et al. 2006). Authorities have used these technologies extensively for “sting” arrests (Wolak et al. 2003b).

Although the technology may be particularly supportive of problematic interactions, the higher risk profile of these technologies may have more to do with who uses these sites and why. Only 18% reported using chatrooms in 2006 (Lenhart et al. 2007a), down from 24% in 2001 (Lenhart et al. 2001). The majority of teens still use instant messaging, but it too has declined in popularity over the same period. Beebe et al. (2004) found that using online chat frequently is correlated with a poor home environment and engaging in other risky behaviors and Ybarra et al. (2005) found a connection between chatroom use and increased depression, suggesting that chat could be a particularly attractive mode of communication for youth who are in need of support and attention. Youth may be more willing to meet strangers through these tools where forums for teens to build relationships are common (Šmahel and Subrahmanyam 2007). Given that risk is highly correlated with certain types of attention seeking and talking with strangers about sexual topics (Wolak et al. 2008a), the youth who participate in chat and the motivations behind their chat use may be more of a factor than the technology itself.

7.2. Blogging

A sizeable minority of youth (28%) have created a blog (Lenhart et al. 2007a), but despite some suggestions that it is potentially dangerous (Huffaker 2006), youth bloggers do not appear to have a higher level of interaction with strangers online and are not more likely to be sexually solicited (Mitchell et al. 2008). That said, they have been found to be more likely to experience online harassment and cyberbullying (Mitchell et al. 2008).

In data collected in 2006, minors aged 12–17 were more likely to be female (Mitchell et al. 2008). Though half of adults who blog do so to network at least some of the times and 34% consider their blogs to be an act of journalism (Lenhart and Fox 2006), teen bloggers blog for an audience of their peers (Lenhart and Madden 2005). Compared to those who use chatrooms, youth bloggers are less likely to send personal information online, engage in online sexual behavior, purposely download pornography, and engage in aggressive online behavior (Mitchell et al. 2008). The fact that they are less likely to be solicited and more likely to face online harassment (Mitchell et al. 2008) may stem from the peer-centric environment of youth participation in blogging.

7.3. Social Network Sites

Social network sites, such as MySpace and Facebook, are one of the most popular and controversial types of social media (boyd and Ellison 2007). Young people are frequently members (Lipsman 2007) and use them to communicate and maintain social relations (boyd 2008) and as a base for online communities (Ito et al. 2008). However, research is inconclusive on the extent to which they present a risk or mediate risk. As of 2006, 93% of American youth aged 12–17 used the Internet, and 58% had created an SNS profile (Lenhart et al. 2007b). Nearly half (49%) of teens used this form of communication to develop new friends (Smith 2007).

With this popularity has come wariness about these types of websites, particularly from parents. In 2007, 85% of adults were uncomfortable with their children participating in online communities (Center for the Digital Future 2008) and in 2006 63% of parents thought there were “quite a few sexual predators” on MySpace; 83% of teens felt that social network sites were generally safe (Rosen 2006). By 2008, 83% of Los Angeles area parents were concerned about sexual predators, yet only 35% of teens felt that predators were a concern (Rosen et al. 2008). Rosen (2008) found that 15% of teens reported being approached by strangers, but almost all (92%) took appropriate steps in response.

Initial research in the UK suggests that at least some minors meet people offline after meeting them on social network sites (Skinner 2008). Although certain SNS members (those who posted a picture and those who flirted online) were more likely to receive online contact from strangers, Smith concluded that, “despite popular concerns about teens and social

networking, our analysis suggests that social network sites are not inherently more inviting to scary or uncomfortable contacts than other online activities” (Smith 2007: 2).

With respect to online harassment, SNSs present an equal or increased danger as compared with other media. Lenhart found that, “social network users are also more likely to be bullied (Lenhart 2007: 4), although this may be a result more of increased (heavy) Internet use and other variables. SNS youth users were also found to be more susceptible to certain types of online harassment, such as spreading of rumors and receiving harassing e-mail (Lenhart 2007). Girls appear to be more prone to receiving unwanted messages on social network sites (Smith 2007). This may be because harassers and solicitors generally target girls or because studies suggest SNS membership is slightly more female (Jones et al. 2008; Thelwall 2008). That said, boys are more likely to see unwanted material such as pornography on SNSs (Rosen et al. 2008).

Privacy features on social network sites are actively employed, leading to increased youth safety. In 2006, Pew found that 66% of youth aged 12–17 had limited access to their SNS profiles (Lenhart and Madden 2007). In other studies, Hinduja found that 40% of MySpace members set their profiles to “private” in 2006 (Hinduja and Patchin 2008b) and 36% in 2007 (Patchin and Hinduja, in review)—a default setting, now, to users who register as under 18. Generally, users appear to realize the need for privacy settings (Lange 2007).

The risks on social network sites—most notably with respect to solicitation and harassment—appear to be consistent with Internet risks more broadly and lower than those in other media (Ybarra and Mitchell 2008). Given the broad popularity of these sites with youth, this suggests that the technology itself plays little role in altering the dynamics of online risk. Furthermore, the profile of those at risk on social network sites matches those who are at risk on the Internet more broadly (Wolak et al. 2008b), suggesting that psychosocial issues are more meaningful markers of risk than technology.

7.4. Multiplayer Online Games and Environments

Nearly all American youth play games daily (Lenhart et al. 2008), many of which have an online component. Of American youth who play games online with others, nearly half (47%) play with friends they know offline, and 27% with people they met online. Contrary to stereotypes, females do play online games, but in lower numbers than males for most genres (Entertainment Software Association 2008; Lenhart et al. 2008; Yee 2006). Youth do not limit

themselves to a single genre, and fully 80% of teens play five or more genres, such as action, sports, racing, and role-playing (Lenhart et al. 2008).

The research is split on whether players of certain games, such as MMOGs (Massively Multiplayer Online Games), are more at risk than other youth with respect to psychosocial factors such as depression, substance abuse, difficulties with self-regulation, trouble at school, and increased aggression (Ducheneaut et al. 2006; Ng and Wiemer-Hastings 2005; Seay and Kraut 2007; Williams and Skoric 2005; Williams et al. 2008). Certain types of online games may represent an attractive outlet for troubled youth, similar to other social media such as chat.

Youth are exposed to violent and sexualized content through video games, as almost one-third (32%) reported playing (Lenhart et al. 2008) at least one mature (“M”)-rated title (Thompson et al. 2006) and even video games with lower ratings contain significant amounts of content that may be considered inappropriate (Haninger and Thompson 2004). It is as yet unclear if the inappropriate content in games is viewed by youth who would not otherwise be exposed to sexualized or violent imagery, and how game playing relates with other activities, such as seeking of adult media through search engines. Youth are also exposed to other forms of problematic content and behavior. Nearly half of game-playing teens report seeing or hearing “people being hateful, racist, or sexist while playing” at least sometimes, and 63% report “people being mean and overly aggressive” (Lenhart et al. 2008).

Online gaming environments frequently have multimedia capabilities and interactive possibilities that go well beyond web-based social media (such as SNSs). Many games offer real-time multimedia chat during gameplay through text, voice, or video, and may encounter aggressive behavior (Williams and Skoric 2005). These introduce the same problematic potential as other forms of synchronous chat. In addition to more familiar modes of communication, three-dimensional environments offer at least one unique way for harassment to occur: “griefing” (Foo and Koivisto 2004). This is defined as when a player “utilizes aspects of the game structure or physics in unintended ways to cause distress for other players” (Warner and Ratier 2005: 47) and disrupts the gaming experience (Lin and Sun 2005).

There is very little research into safety issues with respect to online gaming. It is unclear how frequently youth encounter solicitation or harassment, how other risk factors described in this paper relate to these environments, or if the new methods of harassment that emerge here are more upsetting to youth. More research is necessary.

7.5. Multimedia Communications

Statistics on the overall prevalence of multimedia use in online harassment shows that it is more harmful, but not as widely prevalent as text forms. These multimedia communications may be images and movies created by victims (British Broadcasting Corporation 2006) posted publicly by harassers to embarrass them, “mash-ups” that combine user-generated content with other imagery or videos (Jenkins 2006), or content unrelated to the victim that is designed to disgust or offend. For instance, 6% of youth reported having an embarrassing picture of them posted online without their permission (Lenhart 2007) and 8% reported being a victim of images transmitted over a cell phone (Raskauskas and Stoltz 2007). Harassment involving multimedia images and movies have been found to be particularly distressing (Smith et al. 2008) and this affects a wide variety of different technologies. In addition, 16% of Internet users have reported using a “web cam” (Rainie 2005), but how this synchronous video is used by Internet offenders is not known.

Pornographic images are also used in the “grooming” process of online solicitation, where youth were sent inappropriate images (such as of genitalia or sexual situations), or images are requested from youth. In the N-JOV study, Internet-initiated sex offenders were found to send adult pornography (10%) or child pornography (9%) to victims (Wolak et al. 2004). In a national survey, 4% of youth who use the Internet reported receiving a request for a sexual picture of themselves (but only 1 youth in 1500 complied) (Mitchell et al. 2007c); in a regional study, 7% of students in grades 7–9 in the Rochester, N.Y. area received an online request for a nude picture (McQuade and Sampat 2008). Pornography production in the seduction process may also represent a way for images involving underage sex to propagate online. One in five online child molesters took “sexually suggestive or explicit photographs of victims or convinced victims to take such photographs of themselves or friends” (Wolak et al. 2008b: 120).

As mobile phones increasingly have more powerful still and video cameras, it is likely that issues around multimedia communications will continue to increase, especially with respect to harassment. Ideally, studies on this issue will track harassment levels as newer multimedia devices become available.

8. Future Research

In addition to the topics discussed here, some areas of youth 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 methodologies and standardized measures that can be compared across populations and studies are also needed to illuminate these under-researched topics. Finally, because these risks to youth are rapidly developing, there is a dire need for ongoing large-scale national surveys to synchronously track and quickly report these complex dynamics as they unfold.

8.1. Minor–Minor Solicitation and Sexual Relations

To date, most research has considered bullying and harassment as primarily between similar-aged youths, while solicitation is sexualized communication involving a minor and an adult (frequently with the intent of seduction). However, one national study indicates that nearly half (43%) of minor solicitations are perpetrated by other minors (Wolak et al. 2006) and the majority of solicitations are anonymous, meaning that it is not entirely clear who the perpetrators are. Our focus on adult–minor solicitations often obscures the more frequent practice of minor–minor sexual solicitation.

It also remains unclear how Internet “solicitations” are integrated with offline relationships among similar-aged youth. We need to consider a more holistic perspective when analyzing how romantic relationships and friendships are created, maintained, and terminated, and the emotional implications this has on teens. Many youth use social media to maintain connections with family and friends, which were initiated offline, but some teens develop online relationships, leading to offline meetings for either friendship or romance (Wolak et al. 2006). The concept of meeting “strangers” online may not accurately reflect the online experiences of American youth, as these meetings are increasingly common and don’t contain the nefarious

connotations as seen in the press. The majority of online relationships reported by U.S. youth were similar-aged (70%) and crossed gender lines (71%) (Wolak et al. 2002), and 2% of youth reported romantic online relationships. A large survey of students in New York State found that 14% in grades 10–12 (some of whom may be adult-aged) have accepted an online invitation for an offline meeting, and 14% had invited someone to an offline meeting (McQuade and Sampat 2008). The same individuals who proposed offline meetings were typically the same ones who also accepted offers of meetings, indicating that there is a minority of youth for whom this behavior is normative. Methodologically and terminologically, relying on the term “stranger” is difficult, because two people are not necessarily strangers after interacting together online.

8.2. Problematic Youth-Generated Content

Most content-driven concerns focus on youth accessing adult content that is deemed age-inappropriate. As more and more youth engage in the production of amateur content (Lenhart and Madden 2005), questions emerge about what kind of content they are producing as well as receiving. To what degree are youth contributing to the production of violent, hateful, and sexual content? The rates of the use of multimedia for consensual sexual relations among minors is nearly completely unknown, but seems likely, given the use of images to develop relationships online (Walther et al. 2001), the wide variety of amateur content created and distributed online both privately and publicly (Jacobs 2007), and the presence of sexualized pictures on SNSs such as MySpace (Pierce 2007a). These movies and images may be created during consensual sexual relationships between similar-aged adolescents, for instance, during flirting, which is common (Lenhart 2007; Schiano et al. 2002) or as an outlet for sexual thoughts and development (Atwood 2006; Subrahmanyam and Greenfield 2008). However, they may also constitute a source of underage pornographic material for adults, should it be posted on a website or otherwise distributed, or fodder for future harassment or bullying. Finally, web-based resources that host this content, such as video and image sharing sites, are a challenge to research using traditional quantitative methodologies. Therefore, in addition to clarification of the role of minors in creating this content, much work remains to be performed on rigorous methodologies for collecting online data, and theory for interpreting it.

8.3. Impact on Less-Visible Groups

Although it has been clearly established that girls are particularly more at risk online, the current research has been nearly silent on the impact of Internet crimes on understudied groups such as youth with disabilities and lesbian, gay, bisexual, and transgender (LGBT) youths. About 25% of cases of Internet solicitation in a nationwide survey were found to involve a male youth and a male adult (Wolak et al. 2004). Furthermore, in that study, “most of the Internet-initiated cases involving boys had elements that made it clear victims were gay or questioning their sexual orientations (e.g., meeting offenders in gay-oriented chatrooms)” (Wolak et al. 2008b: 118). All of the youth involved in these online activities may not identify as LGBT later in life, but these studies do identify teens who are questioning their sexuality (LGBT and “straight” alike).

LGBT minors use the Internet for purposes such as creating identities, for friendship, coming out, developing intimate relationships, and for locating communities of others like them (Hiller and Harrison 2007). They may be sensitive to cyberbullying such as ostracizing (Smith and Williams 2004), or more prone to online solicitation (Berson 2003), and have been found to receive more harassing online contact than heterosexual students (in an undergraduate sampling) (Finn 2004). Future studies conducted by Ybarra and other researchers will likely have more measures on LGBT youth and their experiences online, including how they may be using the Internet to meet consensual partners (Ybarra, personal communication, June 26, 2008).

There are no large, quantitative studies of youth with disabilities. Like LGBT youth, these youth may use the Internet to connect to others like them. They may also use the Internet to connect in ways that are simply not possible physically. Too little is currently known about these youth.

8.4. Interplay Between Socioeconomic Class and Risk Factors

The “digital divide” involves complex debates about who does and who does not have Internet access (Hargittai 2002; Martin 2003; van Dijk and Hacker 2003). Recent studies by Pew Internet and American Life Project reveal that 93% of U.S. youth aged 12–17 have some form of Internet access (Lenhart et al. 2007a), but that access is not always equal (Jenkins et al. 2006). At play in all of these discussions is a fundamental question about how socioeconomic status or class interconnects with youth participating in digital culture.

Few studies have examined the relationship between class and specific types of online participation. With respect to social network site adoption, a class-based adoption divide among youth was demonstrated both quantitatively (Hargittai 2007) and qualitatively (boyd 2008). Yet this is an extremely understudied area.

There are no quantitative studies concerning the relationship between class and online risks. This is unfortunate given likely differences in adoption patterns, household dynamics, and educational infrastructure.

8.5. Photographs and Video in Online Harassment and Solicitation

Text is still dominant in much of the current research (Lenhart 2007; Raskauskas and Stoltz 2007), but images and movies may be particularly distressing to victims (Smith et al. 2008) or increase the initial attraction (Walther et al. 2001). Indeed, we already accept elsewhere in this body of research that images of particular content (such as child pornography and hate crime videos) are upsetting. Multimedia-capable mobile devices are gaining in popularity (Center for the Digital Future 2008; Hinduja and Patchin 2009), which offer multimedia recording through an “always-on” connection direct to the Internet. A similar charge can be leveled against research on multimedia harassment as was made against multimedia computer-mediated communication (CMC) in 2000 (Soukup 2000): more research is required to overcome the “text-only bias” of online harassment. Harassment and solicitations are increasingly complex and multimodal, and offenders may integrate, process, and post photographs and videos in ways we don’t yet understand. Special care should be taken to assess the impact of and track this new form of cyberbullying over the next several years.

8.6. Intersection of Different Mobile and Internet-based Technologies

The majority (77%) of Internet-initiated sex crimes against youth used multiple modes of communication (Wolak et al. 2004), but little is understood about the interplay between them. Furthermore, most research to date focuses on the role of the Internet, but mobile phones are increasingly playing a role in sexual solicitation, harassment, and access to problematic content. It is already known that mobile phone use is a risk factor for receiving aggressive sexual solicitations online (Mitchell et al. 2007b) and online harassment (Hinduja and Patchin 2009).

How mobile devices are used in the United States for harassment and solicitation requires further examination over the next several years as these devices are adopted and come into mainstream use.

8.7. Online Activities of Registered Sex Offenders

No laws prevent registered sex offenders from participating in social media, but many people are concerned about their participation and the potential risk it poses to youth. There are no studies that concern the activities of registered sex offenders online, whether their participation in social media is correlated with increased risk, or whether they use social media to contact youth more than other channels. Much more research is necessary to determine whether registered sex offenders pose a threat to youth through their online activities.

8.8. Continued Research, New Methodologies, and Conceptual Clarity

There is a dire need for more research on Internet risks to youth, particularly quantitative studies involving a representative sampling of Americans, and those with a meaningful qualitative dimension. Longitudinal research involving repeated measures is scarce (Center for the Digital Future 2008; Lenhart 2007; Wolak et al. 2006). Continued large-scale surveys and meta-analyses are required to gain an increased understanding of incidence rate, risk factors, and characteristics of threats. It is also important for us to understand how adults view the risks to youth, and how youth see the role and risks of social media. Currently, “less research is qualitative or multi-method in nature, so we have less knowledge of children’s own experiences or perceptions, or of the ways in which online activities are contextualized within their everyday lives” (Livingstone and Haddon 2008: 317).

As further research is conducted, our understanding of the activities of online perpetrators, victims, and participants is likely to change. The current concept of minors meeting “strangers” online, leading to real-world meetings, is too simple a perspective. Youth use various media to create and maintain friendships, whether they have their origins offline or online. Less attention should be placed on Internet-*initiated* relationships, and more on Internet-*maintained* ones. Little is known about the activities of how offline sexual interactions involve SNSs, or how registered sex offenders use these sites, for example.

Standardization of concepts would be useful to compare data across studies. For instance, as previously noted, age-related cyberbullying findings are difficult to compare, as studies alternately collect and report age with large ranges (such as “older adolescents”), smaller ranges (such as 12–13 years old), exact age (in years), and grade number (which corresponds only loosely to age). Reports of cyberbullying vary across the schools and districts from which participants are frequently recruited from (Kowalski and Limber 2007; Raskauskas and Stoltz 2007) as do the durations of the harassment under investigation (Moessner 2007; Smith et al. 2008).

Finally, there is clearly a need for a more rapid processing and delivery of results. There is currently a dearth of academically rigorous, peer-reviewed online journals, particularly those that make data sets available for secondary analysis. Any study of how youth use and integrate technologies in their everyday lives is a snapshot of a moving target, and we must keep up. As Livingstone and Haddon note, “research in this field becomes quickly out of date, as the technologies, institutions that promote and manage them, and children’s own practices all continue to change” (Livingstone and Haddon 2008: 317).

9. Understanding Research Methodologies (Appendix A)

This appendix provides a brief overview of research methodologies that assist in the understanding of the studies included in this document, particularly terminology and concepts that provide an understanding of the limitations of this research. The purposes of quantitative research are to help explain, add to our understanding, and predict (Kerlinger and Lee 1999). This paper focuses on quantitative, national-level studies with a large sample size, but includes studies that vary by methodology (qualitative or quantitative), sample size (number of participants), location, funding source, and administration method.

9.1. Samplings

A *probability* sampling will typically select its users at random from a sampling *frame* (list of potential participants), such as a list of all the home phone numbers in the United States. This sampling is generally preferred in quantitative research, particularly a *representative* sampling, which refers to a group of participants that is a miniature of the population (Shadish et al. 2001). For instance, an ideal research population would mirror the gender and racial makeup of the population to which the findings are *generalized* (also known as having *external validity*). Few studies in this paper claim a representative national sampling of Americans.

The reasons that representative samplings are comparatively rare is that (1) the population under research may not be known (making the sampling by definition *nonprobability*), (2) ethical restrictions prohibit collection of data from underage populations without parental approval, and (3) national studies are expensive and difficult to conduct. They are expensive because they require that phone calls be made and voice interviews conducted, or paper surveys sent out and the results processed. They are difficult to conduct because research involving underage subjects is typically not as easy to clear, particularly through the Institutional Review Boards (IRBs) that exist at most research institutions to guarantee that studies are conducted in a safe and ethical manner. Additionally, in some cases, the topic under study may be impossible to research in any meaningful way using a national survey. Researching the prevalence of solicitation of youth is one example: few Americans would admit to this blatantly illegal activity. In this case, the only way to examine the national prevalence of online solicitations with a probability, national, sampling frame is by surveying youth and asking them

how frequently they were solicited (Wolak et al. 2006). The challenge of collecting meaningful information on these incidents has been called a “tip of the iceberg” problem, where the number of reported offenses might be much lower than the actual number of offenders (Sheldon and Howitt 2007: 43).

Localized studies are more common, and generally use smaller groups of participants, termed *convenience* samplings, because the population is easily available. This sampling may be of a selection of youth in certain grades across several schools (Li 2005), school systems (McQuade and Sampat 2008), or certain grades in a statewide survey. Additionally, research may be conducted entirely online and not relate directly to any physical location (Fielding et al. 2008). A convenience sampling is probably easier to collect data from, and may have a larger participation rate, as youth are more likely to take part in a survey conducted by a teacher or researcher whom they’ve met than participate in a phone- or computer-based survey in which researchers are remote and nonvisible. Convenience samplings are not necessarily a problem, as long as the researchers are aware of the lack of generalizability of their results (Shadish et al. 2001).

Another common recruiting method online is a snowball sampling, which is a group of users selected by asking participants to recommend their friends. Many researchers find this a convenient and effective way to recruit participants from social network sites (Rosen 2006), MMOGs (Lin and Sun 2005) and blogs (Faulkner and Melican 2007). It is difficult to claim a representative sampling using a snowball method, as the participants vary depending on the social networks of the group under research and how they forward requests to others. Rothenburg notes that “in the absence of a probability sample . . . desirable statistical properties are not available to the investigator. The subsequent use of statistical tests that rest on assumptions of random sampling from a known underlying distribution is problematic. The absence of a statistical cornerstone has been a concern of investigators in the field and a source of skepticism for those in other disciplines” (1995: 106). This does not mean that these types of studies aren’t valuable in advancing our understanding of online safety, but merely that it is difficult to make inferences to a larger population via this collection method.

9.2. Response Rates

Different administration methods have different response rates (Sue and Ritter 2007). A survey, for instance, may be administered via phone (Wolak et al. 2006), on paper (Li 2007b), or

on a computer (McQuade and Sampat 2008). Because it is not ethical to force an individual to participate in research, individuals who are contacted may elect not to participate, or (typically) discontinue involvement in the research at any time. This leads to lower response rates. The less likely individuals are to respond and participate in the survey through a given medium, the lower the response rate. Online surveys, for instance, have the lowest response rate (Sue and Ritter 2007), as most Internet users are saturated with emails and just ignore the invitation to participate. In addition to these *cooperation* and *completion* rates, phone surveys that don't draw on a sampling frame (such as a phonebook) are also subject to a lower *contact* rate due to the dialing of inactive numbers (Lenhart et al. 2008). The advantage of this method is that all phones are in the sampling frame, including cell phones.

9.3. Prevalence

The prevalence and character of online threats to youth will be examined throughout this document. The *overall* prevalence of these threatening acts and problematic content remains difficult to estimate, because (1) there is no government body collecting statistics on online child abuse (Finkelhor 2008) or harassment; (2) offenders are mostly unavailable to research (a goal is to evade capture); (3) minors may be unlikely to speak out about sensitive issues such as harassment (DeHue et al. 2008; Slonje and Smith 2008) or solicitation (Mitchell et al. 2004) to parents, teachers, or police; (4) statistics on certain types of offenses (such as possession of child pornography) nearly universally involve data from offenders in various stages of prosecution or incarceration, biasing the data; (5) as previously mentioned, many of these activities are not illegal, and therefore not frequently reported; and (6) the Internet provides an extremely high degree of connectivity along with low levels of identifying information. Given the challenge of collecting meaningful information on these crimes, some have argued that—similar to sex crimes in general—the number of reported Internet-based offenses is much lower than the actual number (Sheldon and Howitt 2007: 43).

9.4. Sources of Bias

There are many sources of *bias* in both qualitative and quantitative research. Bias is defined as “systematic error in an estimate or an inference” (Shadish et al. 2001: 505), and can take many forms, some of which we will cover here. A related issue to administration medium and sampling method is self-selection bias, which occurs when participants are allowed to control whether they participate. If those who choose to participate are different than those who don’t want to participate, inaccurate results emerge. Unfortunately, self-selection bias is a caveat in most studies considered here (except for content analyses or meta-analyses, which involve the use of secondary data), as it is typically considered to be unethical to force participants to participate in research. Reasonable coercive methods may be employed such as a lottery, small payment, or small gift. Other threats to internal validity imposed by participants include social expectations, where participants give answers they believe are more in line with social norms, particularly for sensitive topics such as pornography or drug use (which they would be inclined to deny). These threats may be addressed by well-designed studies, such as double-blind administration.

9.5. Constructs

As with many new areas of research, many definitions have been proposed for *constructs* (or concepts) under study. There is no standard accepted definition for cyberbullying, solicitation, or offensive content. Constructs used in the studies in this paper have emerged from various disciplines, including developmental psychology, interpersonal communication, and mass communication. Each discipline has a particular perspective it brings. To a degree, this is positive, as it drives a healthy debate over how and why modes of interaction online present risk to youth. In other ways, varying constructs presents a challenge, because data from various studies are difficult to compare. Also, if a construct is faulty, a study is at risk for construct validity. As previously discussed, solicitation encompasses a variety of contact, including sexual harassment, flirting, and online seduction. If two studies defined solicitation differently, then the two studies have an issue of external validity. In other words, they may be comparing apples and oranges.

9.6. Question Wording

The process of creating a question to collect responses relating to a concept is known as *operationalizing* it. In addition to disparity in concepts, the wording used to operationalize questions varies between studies, producing sources of variation. These points of variance explain in part why certain statistics vary greatly, such as the wide disparity in reported cyberbullying (4%–46%). For example, McQuade and Sampat (2008) use age-appropriate language to capture aspects of cyberbullying in different age groups. These researchers preferred to collect information about various behaviors that are perhaps related to cyberbullying, but did not predefine cyberbullying as a set of behaviors. In this way, “interpreters of the data are left to draw their own conclusions about the nature and extent of cyberbullying, as well as other types of online behaviors” (S. McQuade, personal communication, November 5, 2008). By comparison, Li (2007a) collects cyberbullying with a much more detailed, paragraph-long definition of what cyberbullying is, then asks questions using that terminology: “I have been cyberbullied (e.g., via email, chat room, cell phone).” There are benefits as well as drawbacks to each of these methods, but naturally, different wordings and research instruments will result in widely varying statistics on the prevalence of cyberbullying. Clearly defined constructs would also address the confusion surrounding the wording of questions.

9.7. Causality and Complexity

Simply put, when an event can be said to lead to a specific effect, this is *causality*. Causality typically cannot generally be inferred from the reviewed studies, for several reasons. A survey or single study cannot by itself “prove” why an observed effect occurs, as can be said of a mathematical equation. In a larger sense, “proving” concepts does not have relevance for social sciences as it does in sciences such as physics, which directly measures empirical truths. Many of the larger questions in communications or psychological research, such as “Does violent media exposure lead to violent actions?” remain a subject of dispute even after decades of study. What is more common is a *correlation*: finding that two variables are related, but also that neither can be said to cause the other. For instance, people who are tall also tend to weigh more. These are simply two variables that are linked due to the size of an individual. Compounding this issue is that online communication is extremely complex. Youth use increasing numbers and

types of social technologies in combination, and it is difficult to isolate the variance of a single effect. Advanced techniques (such as computer modeling) can be said to account for such variance, but they do not necessarily increase the ability for a researcher to claim causality.

9.8. Qualitative Methodologies

A different kind of study, which is referenced sparingly in this paper, is the qualitative study (Berg 2004). This type of research typically focuses on in-depth analysis of a smaller group of subjects, analyzing intrinsic meaning of their activities. It is theoretically distinct from quantitative research, but informs our understanding of how these individuals operate. For instance, interviews can be used to discuss how offenders integrate pornography into their online habits (Frei et al. 2005) and focus groups on the topic of how youth encounter sexualized media on the Internet (Cameron et al. 2005). Both of these are topics and groups that would be difficult to research using quantitative methodologies, and led to richer sets of data to inform areas of investigation. The question of whether these populations can be extrapolated to larger populations is moot with qualitative research, as it does not reference an empirical reality, generally uses words instead of numbers as the units of analysis, and uses vastly different data collections methods (such as focus groups, interviews, and immersive ethnographic research). “Mixed-methods” research—quantitative and qualitative research applied together—also exists, although it appears extremely infrequently in the research compiled in this paper.

Qualitative research is quite beneficial for understanding the topology of a domain. Many of the scholars cited in this review work with qualitative scholars or do qualitative research before organizing their survey. Qualitative work like ethnography can surface important topics that have not yet been considered analytically by quantitative scholars. Many of the suggestions for future research stem from issues surfaced in qualitative work, such as the ethnographic studies funded by the MacArthur Foundation (Ito et al. 2008).

9.9. Funding Sources

Many studies, particularly national surveys that are expensive to conduct, receive some form of funding. Funding generally will be disclosed in a published, peer-reviewed article. For instance, the YISS-1 and YISS-2 surveys were funded by the U.S. Department of Justice. This

affiliation is disclosed on the first page of some reports (Wolak et al. 2006) and at the end of others, prior to the references (Wolak et al. 2007c). It is common for larger studies to require some financial backing. Though it does not mean that the researchers are necessarily biased, it is ethical for them to disclose such affiliations.

9.10. Underreporting of Incidents

The small number of successful online solicitations by adults of children or adolescents defies examination with a survey, because the incident rate is so low, and because both perpetrators and victims are unlikely to report such activities to parents or authorities. Similarly, adults are unlikely to disclose information on their online consumption of child pornography, and minors may be ashamed to admit to nonconsensual or consensual sexual situations that occurred. Creative ways of recruiting and examining inaccessible populations are needed, such as examining how the Internet is integrated into incidents of minor–minor forcible sex by using data collected from rape crisis center volunteers.

10. References

- Adam, Alison. 2002. "Cyberstalking and Internet pornography: Gender and the gaze." *Ethics and Information Technology* 4(2): 133–142.
- Agatston, Patricia W., Robin Kowalski, and Susan Limber. 2007. "Students' Perspectives on Cyber Bullying." *Journal of Adolescent Health* 41:S59–S60.
- American Psychological Association. 2000. *Diagnostic and Statistical Manual of Mental Disorders*. Arlington, VA: American Psychiatric Publishing.
- Arnaldo, Carlos A. 2001. *Child Abuse on the Internet: Ending the Silence*. Paris, France: Berghahn Books.
- Atwood, Joan D. 2006. "Mommy's Little Angel, Daddy's Little Girl: Do You Know What Your Pre-Teens Are Doing?" *The American Journal of Family Therapy* 34:447–467.
- Bancroft, John. 2003. *Sexual Development in Childhood*. Bloomington, IN: Indiana University Press.
- Barnow, Sven, Michael Lucht, and Harald-J. Freyberger. 2001. "Influence of Punishment, Emotional Rejection, Child Abuse, and Broken Home on Aggression in Adolescent: An Examination of Aggressive Adolescents in Germany." *Psychopathology* 34(4): 167–173.
- Beebe, Timothy J., Stephen E. Asche, Patricia A. Harrison, and Kathryn B. Quinlan. 2004. "Heightened Vulnerability and Increased Risk-Taking Among Adolescent Chat Room Users: Results From a Statewide School Survey." *Journal of Adolescent Health* 35:116–123.
- Bensimon, Philippe. 2007. "The Role of Pornography in Sexual Offending." *Sexual Addiction & Compulsivity* 14(2): 95–117.
- Beran, Tanya and Qing Li. 2007. "The Relationship between Cyberbullying and School Bullying." *Journal of Student Wellbeing* 1(2): 15–33.
- Berg, Bruce L. 2004. *Qualitative Research Methods for the Social Sciences (Fifth edition)*. Allyn & Bacon/Pearson. Boston, MA.
- Berrier, Tonya. 2007. "Sixth-, Seventh-, and Eighth-Grade Students' Experiences with the Internet and Their Internet Safety Knowledge." Educational Leadership and Policy Analysis, East Tennessee State University.
- Berson, Ilene R. 2003. "Grooming Cybervictims: The Psychosocial Effects of Online Exploitation for Youth." *Journal of School Violence* 2(1): 5–18.
- Berson, Ilene R. and Michael J. Berson. 2005. "Challenging Online Behaviors of Youth: Findings From a Comparative Analysis of Young People in the United States and New Zealand." *Social Science Computer Review* 23(1): 29–38.

- Biber, Jodi K., Dennis Doverspike, Daniel Baznik, Alana Cober, and Barbara A. Ritter. 2002. "Sexual Harassment in Online Communications: Effects of Gender and Discourse Medium." *CyberPsychology & Behavior* 5(1): 33–42.
- Borg, Mark G. 1998. "The Emotional Reaction of School Bullies and their Victims." *Educational Psychology* 18(4): 433–444.
- boyd, danah. 2008. "Taken out of context: American Teenage Socialization in Networked Publics." PhD Thesis, School of Information, University of California, Berkeley, CA.
- boyd, danah and Nicole Ellison. 2007. "Social Network Sites: Definition, History, and Scholarship." *Journal of Computer-Mediated Communication* 13(1).AU: PAGE RANGE?
- Brendgen, Mara, Frank Vitaro, Richard E. Tremblay, and Francine Lavoie. 2001. "Reactive and Proactive Aggression: Predictions to Physical Violence in Different Contexts and Moderating Effects of Parental Monitoring and Caregiving Behavior." *Journal of Abnormal Child Psychology* 29(4): 293–304.
- Briere, John and Marsha Runtz. 1989. "University Males' Sexual Interest in Children: Predicting Potential Indices of "Pedophilia" in a Nonforensic Sample." *Child Abuse & Neglect* 13:65–75.
- British Broadcasting Corporation. 2006. "Star Wars Kid is top viral video." *BBC News*, 27 November. (<http://news.bbc.co.uk/2/hi/entertainment/6187554.stm>).
- Brookshire, Malena and Christine Maulhardt. 2005. "Evaluation of the Effectiveness of the NetSmartz Program: A Study of Maine Public Schools." NetSmartz, August 22. (http://www.netsmartz.org/pdf/gw_evaluation.pdf).
- Bryn, Robert J. and Rhonda L. Lenton. 2001. "Love Online: A Report on Digital Dating in Canada." MSN.ca, February 6. (<http://www.nelson.com/nelson/harcourt/sociology/newsociety3e/loveonline.pdf>).
- Burgess-Proctor, Amanda, Justin Patchin, and Sameer Hinduja. 2009. "Cyberbullying and online harassment: Reconceptualizing the victimization of adolescent girls." in *Female crime victims: Reality reconsidered*, edited by V. Garcia and J. Clifford. Upper Saddle River, NJ: Prentice Hall.
- Calpin, Christine M. 2006. "Child Maltreatment." U.S. Department of Health & Human Services, (<http://www.acf.hhs.gov/programs/cb/pubs/cm06/cm06.pdf>).
- Cameron, Kenzie A., Laura F. Salazar, Jay M. Bernhardt, Nan Burgess-Whitman, Gina M. Wingood, and Ralph J. DiClemente. 2005. "Adolescents' experience with sex on the web: results from online focus groups." *Journal of Adolescence* 28(4): 535–540.
- Center for the Digital Future. 2008. "Annual Internet Survey by the Center for the Digital Future Finds Shifting Trends Among Adults About the Benefits and Consequences of Children Going Online." (http://www.digitalcenter.org/pages/current_report.asp?intGlobalId=19).

- Chau, Michael and Jennifer Xu. 2007. "Mining communities and their relationships in blogs: A study of online hate groups." *International Journal of Human-Computer Studies* 65(1): 57–70.
- Cho, Chang-Hoan and Hongsik John Cheon. 2005. "Children's Exposure to Negative Internet Content: Effects of Family Context." *Journal of Broadcasting & Electronic Media* 49(4): 488–509.
- Computer Science and Telecommunications Board National Research Council. 2002. *Youth, Pornography, and the Internet*, Edited by Dick Thornburgh and Herbert Lin. National Academies Press.
- de Zengotita, Thomas. 2006. *Mediated: How the Media Shapes Our World and the Way We Live in It*. Bloomsbury USA. New York, NY.
- DeHue, Francine, Catherine Bolman, and Trijntje Völlink. 2008. "Cyberbullying: Youngsters' Experiences and Parental Perception." *CyberPsychology & Behavior* 11(2): 217–223.
- Deirmenjian, John M. 2000. "Hate Crimes on the Internet." *Journal of Forensic Sciences* 45(5): 1020–1022.
- Devoe, Jill F., Katharin Peter, Margaret Noonan, Thomas D. Snyder, Katrina Baum, and Thomas D. Snyder. 2005. "Indicators of School Crime and Safety: 2005." U.S. Department of Justice, November. (<http://www.ncjrs.gov/App/publications/abstract.aspx?ID=210697>).
- Ducheneaut, Nicolas, Nicholas Yee, Eric Nickell, and Robert J. Moore. 2006. "'Alone Together?' Exploring the Social Dynamics of Massively Multiplayer Online Games." Proceedings of *SIGCHI*: 407–416.
- Eastin, Matthew S., Bradley S. Greenberg, and Linda Hofschire. 2006. "Parenting the Internet." *Journal of Communication* 56(3): 486–504.
- Entertainment Software Association. 2008. "2008 Sale, Demographic and Usage Data: Essential Facts about the Computer and Video Game Industry." (http://www.theesa.com/facts/pdfs/ESA_EF_2008.pdf).
- Ericson, Nels. 2001. "Addressing the Problem of Juvenile Bullying." *OJJDP Fact Sheet* 27. (<http://www.ncjrs.org/pdffiles1/ojjdp/fs200127.pdf>).
- Faulkner, Susan and Jay Melican. 2007. "Getting Noticed, Showing-Off, Being Overheard: Amateurs, Authors and Artists Inventing and Reinventing Themselves in Online Communities." Paper presented at the *Ethnographic Praxis in Industry*, Paris.
- Fielding, Nigel G., Raymond M. Lee, and Grant Blank. 2008. *The Handbook of Online Research Methods*. Sage. Thousand Oaks, CA.
- Finkelhor, David. 2008. *Childhood Victimization: Violence, Crime, and Abuse in the Lives of Young People*. New York, NY: Oxford University Press.

- Finkelhor, David and Lisa Jones. 2008. "Updated Trends in Child Maltreatment, 2006." Crimes Against Children Research Center. (<http://www.unh.edu/ccrc/Trends/index.html>).
- Finkelhor, David, Kimberly J. Mitchell, and Janis Wolak. 2000. "Online Victimization: A Report on the Nation's Youth." National Center for Missing and Exploited Children, June. (<http://www.unh.edu/ccrc/pdf/jvq/CV38.pdf>).
- Finkelhor, David and Richard Ormrod. 2000. "Kidnaping of Juveniles: Patterns from NIBRS." Office of Juvenile Justice and Delinquency Prevention, June. (<http://www.ncjrs.org/pdffiles1/ojjdp/181161.pdf>).
- Finn, Jerry. 2004. "A Survey of Online Harassment at a University Campus." *Journal of Interpersonal Violence* 19(4): 468–483.
- Fleming, Michele and Debra Rickwood. 2004. "Teens in Cyberspace: Do they encounter friend or foe?" *Youth Studies Australia* 23(3): 46–52.
- Fleming, Michele J., Shane Greentree, Dayana Cocotti-Muller, Kristy A. Elias, and Sarah Morrison. 2006. "Safety in Cyberspace: Adolescents' Safety and Exposure Online." *Youth & Society* 38(2): 135–154.
- Flood, Michael. 2007. "Exposure to pornography among youth in Australia." *Journal of Sociology* 43(1): 45–60.
- Foo, Chek Yang and Elina M. I. Koivisto. 2004. "Defining grief play in MMORPGs: player and developer perceptions." Proceedings of *SIGCHI*, Vienna: ACM, 245–250.
- Frei, Andreas, Nuray Erenay, Volker Dittmann, and Marc Graf. 2005. "Paedophilia on the Internet—a study of 33 convicted offenders in the Canton of Lucerne." *Swiss Medical Weekly* 135(33/34): 488–494.
- Fulda, Joseph F. 2002. "Do Internet Stings Directed at Pedophiles Capture Offenders or Create Offenders? And Allied Questions." *Sexuality & Culture* 6(4): 73–100.
- Fulda, Joseph S. 2007a. "Internet Stings Directed at Pedophiles: A Study in Philosophy and Law." *Sexuality & Culture* 11(1): 52–98.
- Fulda, Joseph S. 2007b. "Update to 'Do Internet Stings Directed at Pedophiles Capture Offenders or Create Offenders? And Allied Questions.'" *Sexuality & Culture* 11(1): 99–110.
- Gennaro, Corinna D. and William H. Dutton. 2007. "Reconfiguring Friendships: Social Relationships and the Internet." *Information, Communication & Society* 10(5): 591–618.
- Patterson, Gerald R. and Philip A. Fisher. 2002. "Recent developments in our understanding of parenting: Bidirectional effects, causal models, and the search for parsimony." In *Handbook of parenting: Vol. 5. Practical issues in parenting*, edited by M. H. Bornstein, 58–88. Mahwah, NJ: Erlbaum.

- Gerstenfeld, Phyllis B., Diana R. Grant, and Chau-Pu Chiang. 2003. "Hate Online: A Content Analysis of Extremist Internet Sites." *Analyses of Social Issues and Public Policy* 3(1): 29–44.
- Glassner, Barry. 1999. *The Culture of Fear*. New York: Penguin.
- Greenfield, Patricia M. 2004. "Inadvertent exposure to pornography on the Internet: Implications of peer-to-peer file-sharing networks for child development and families." *Journal of Applied Developmental Psychology* 25(6): 741–750.
- Griffiths, M. D., Mark N. O. Davies, and Darren Chappell. 2004. "Online computer gaming: a comparison of adolescent and adult gamers." *Journal of Adolescence* 27(1): 87–96.
- Gross, Elisheva F. 2004. "Adolescent Internet use: What we expect, what teens report." *Applied Developmental Psychology* 25: 633–649.
- Hall, Gordon C. Nagayama, Richard Hirschman, and Lori L. Oliver. 1995. "Sexual Arousal and Arousability to Pedophilic Stimuli in a Community Sample of Normal Men." *Behavior Therapy* 26(4).
- Hancock, Jeff, Catalina Toma, and Nicole Ellison. 2007. "The Truth About Lying in Online Dating Profiles." Proceedings of *CHI 2007*, San Jose: ACM.
- Haninger, Kevin and Kimberly M. Thompson. 2004. "Content and Ratings of Teen-Rated Video Games." *Journal of the American Medical Association* 291(7): 856–865.
- Hargittai, Eszter. 2002. "Second-Level Digital Divide: Differences in People's Online Skills." *First Monday* 7(4): 1–20.
- Hargittai, Eszter. 2007. "Whose Space? Differences Among Users and Non-Users of Social Network Sites." *Journal of Computer-Mediated Communication* 13(1): article 14.
- Hartmann, Tilo and Christoph Klimmt. 2006. "Gender and Computer Games: Exploring Females' Dislikes." *Journal of Computer Mediated Communication* 11: 910–913.
- Hasebrink, Uwe, Sonia Livingstone, and Leslie Haddon. 2008. "EU Kids Online: Comparing children's online opportunities and risks across Europe." (<http://www.lse.ac.uk/collections/EUKidsOnline/Reports/Default.htm>).
- Hawker, David S. J. and Michael J. Boulton. 2000. "Twenty years' Research on Peer Victimization and Psychosocial Maladjustment: A Meta-analytic Review of Cross-sectional Studies." *Journal of Child Psychology and Psychiatry* 41(4): 441–455.
- Haynie, Denise L., Tonja Nansel, Patricia Eitel, Aria Davis Crump, Keith Saylor, Kai Yu, and Bruce Simons-Morton. 2001. "Bullies, Victims, and Bully/Victims: Distinct Groups of At-Risk Youth." *The Journal of Early Adolescence* 21(1): 29–49.
- Hiller, Lynne and Lyn Harrison. 2007. "Building Realities Less Limited Than Their Own: Young People Practising Same-Sex Attraction on the Internet." *Sexualities* 10(1): 82–100.

- Hinduja, Sameer and Justin Patchin. 2007. "Offline Consequences of Online Victimization: School Violence and Delinquency." *Journal of School Violence* 6(3): 89–112.
- Hinduja, Sameer and Justin Patchin. 2008a. "Cyberbullying: An Exploratory Analysis of Factors Related to Offending and Victimization." *Deviant Behavior* 29(2): 129–156.
- Hinduja, Sameer and Justin Patchin. 2008b. "Personal information of adolescents on the Internet: A quantitative content analysis of MySpace." *Journal of Adolescence* 31:125–146.
- Hinduja, Sameer and Justin Patchin. 2009. *Bullying Beyond the Schoolyard: Preventing and Responding to Cyberbullying*. Thousand Oaks, CA: Sage.
- Hines, Denise A. and David Finkelhor. 2007. "Statutory sex crime relationships between juveniles and adults: A review of social scientific research." *Aggression and Violent Behavior* 12:300–314.
- Hoffman, Donna L. and Thomas P. Novak. 1995. "A Detailed Analysis of the Conceptual, Logical, and Methodological Flaws in the Article: 'Marketing Pornography on the Information Superhighway.'" Retrieved August 23, 2008. (http://w2.eff.org/Censorship/Rimm_CMU_Time/rimm_hoffman_novak.critique).
- Howitt, Dennis and Kerry Sheldon. 2007. "The role of cognitive distortions in paedophilic offending: Internet and contact offenders compared." *Psychology, Crime & Law* 13(5): 469–486.
- Huffaker, David. 2006. "Teen Blogs Exposed: The Private Lives of Teens Made Public." Proceedings of *American Association for the Advancement of Science*. AU VOL/ISS/DATE/PAGE?
- International Centre for Missing & Exploited Children. 2006. "Child Pornography: Model Legislation & Global Review." (http://www.icmec.org/en_X1/pdf/ModelLegislationFINAL.pdf).
- Ito, Mizuko, Sonja Baumer, Matteo Bittanti, danah boyd, Rachel Cody, Becky Herr-Stephenson, Heather A. Horst, Patricia G. Lange, Dilan Mahendran, Katynka Martinez, C.J. Pascoe, Dan Perkel, Laura Robinson, Christo Sims, and Lisa Tripp. 2008. "Hanging Out, Messing Around and Geeking Out: Living and Learning with New Media." MacArthur Foundation, November 20. (<http://digitalyouth.ischool.berkeley.edu/report>).
- Jacobs, Katrien. 2007. *Netporn: DIY Web Culture and Sexual Politics (Critical Media Studies)*. Lanham, MD: Rowman & Littlefield Publishers, Inc.
- Jaishankar, K., Debarati Halder, and S. Ramdoss. 2008. "Pedophilia, Pornography, and Stalking: Analyzing Child Victimization on the Internet." In *Crimes of the Internet*, edited by F. Schmallerger, & Pittaro, M, 28–42. Upper Saddle River, NJ: Prentice Hall.
- Jenkins, Henry. 2006. *Convergence Culture*. New York: New York University Press.
- Jenkins, Henry, Katie Clinton, Ravi Purushotma, Alice J. Robinson, and Margaret Weigel. 2006. "Confronting the Challenges of Participatory Culture: Media Education for the 21st Century." MacArthur Foundation. (<http://www.newmedialiteracies.org/files/working/NMLWhitePaper.pdf>).

- Jenkins, Philip. 2001. *Beyond Tolerance: Child Pornography Online*. New York: New York University Press.
- Jenkins, Philip. 2003. *Beyond Tolerance: Child Pornography on the Internet*. New York: New York University Press.
- Jones, Steve, Sarah Millermaier, Mariana Goya-Martinez, and Jessica Schuler. 2008. "Whose space is MySpace? A content analysis of MySpace profiles." *First Monday* 13(9).
- Kerlinger, Fred N. and Howard B. Lee. 1999. *Foundations of Behavioral Research*. Florence, KY: Wadsworth Publishing.
- Keski-Rahkonen, Anna and Federica Tozzi. 2005. "The Process of Recovery in Eating Disorder Sufferers' Own Words: An Internet-Based Study." *International Journal of Eating Disorders* 37:S80–S86.
- Kim, Candice. 2005. "From Fantasy to Reality: The Link Between Viewing Child Pornography and Molesting Children." *Prosecutor* 39(2): 17–18, 20, 47.
- Kowalski, Robin M. and Susan P. Limber. 2007. "Electronic Bullying Among Middle School Students." *Journal of Adolescent Health* 41:S22–S30.
- Kowalski, Robin M., Susan P. Limber, and Patricia W. Agatston. 2007. *Cyber Bullying: Bullying in the Digital Age*. Malden, MA: Wiley-Blackwell.
- Lamb, Michael. 1998. "Cybersex: Research Notes on the Characteristics of Visitors to Online Chat Rooms." *Deviant Behavior* 19:121–135.
- Lang, Reuben A. and Roy R. Frenzel. 1988. "How Sex Offenders Lure Children." *Annals of Sex Research* 1(2): 303–317.
- Lange, Patricia G. 2007. "Publicly private and privately public: Social networking on YouTube." *Journal of Computer-Mediated Communication* 13(1).
- Lee, Elissa and Laura Leets. 2002. "Persuasive Storytelling by Hate Groups Online." *American Behavioral Scientist* 45(6): 927–957.
- Leets, Laura. 2001. "Responses to Internet Hate Sites: Is Speech Too Free in Cyberspace?" *Communication Law and Policy* 6(2): 287–317.
- Lenhart, Amanda. 2007. "Cyberbullying and Online Teens." Pew Internet & American Life Project, June 27. (http://www.pewinternet.org/PPF/r/216/report_display.asp).
- Lenhart, Amanda and Susannah Fox. 2006. "Bloggers: A portrait of the Internet's new storytellers." Pew Internet & American Life Project, July 19. (http://www.pewinternet.org/PPF/r/186/report_display.asp).

- Lenhart, Amanda, Joseph Kahne, Ellen Middaugh, Alexandra Rankin Macgill, Chris Evans, and Jessica Vitak. 2008. "Teens, Video Games, and Civics." Pew Internet & American Life Project, September 16. (http://www.pewinternet.org/PPF/r/263/report_display.asp).
- Lenhart, Amanda and Mary Madden. 2005. "Teen Content Creators and Consumers." Pew Internet and American Life Project, November 2. (http://www.pewinternet.org/ppf/r/166/report_display.asp).
- Lenhart, Amanda and Mary Madden. 2007. "Teens, Privacy, & Online Social Networks." Pew Internet and American Life Project, April 18. (http://www.pewinternet.org/PPF/r/211/report_display.asp).
- Lenhart, Amanda, Mary Madden, Alexandra R. Macgill, and Aaron Smith. 2007a. "Teens and Social Media." Pew Internet & American Life Project, December 19. (http://www.pewinternet.org/PPF/r/230/report_display.asp).
- Lenhart, Amanda, Mary Madden, Alexandra R. Macgill, and Aaron Smith. 2007b. "Writing, Technology and Teens." Pew Internet & American Life Project, December 19. (http://www.pewinternet.org/pdfs/PIP_Teens_Social_Media_Final.pdf).
- Lenhart, Amanda, Lee Rainie, and Oliver Lewis. 2001. "Teenage Life Online: The Rise of the Instant-message Generation and the Internet's Impact on Friendships and Family Relationships." Pew Internet & American Life Project, June 21. (http://www.pewinternet.org/report_display.asp?r=36).
- Levine, Judith. 2002. *Harmful to minors*. Minneapolis: University of Minnesota Press.
- Li, Qing. 2005. "Cyber-bullying in schools: Nature and extent of adolescents' experience." Presented at *American Educational Research Association*, Montreal: April 21.
- Li, Qing. 2006. "Cyberbullying in Schools: A Research of Gender Differences." *School Psychology International* 27(2): 157–170.
- Li, Qing. 2007a. "Bullying in the new playground: Research into cyberbullying and cyber victimisation." *Australasian Journal of Educational Technology* 23(4): 435–454.
- Li, Qing. 2007b. "New bottle but old wine: A research of cyberbullying in schools." *Computers in Human Behavior* 23:1777–1791.
- Liau, Albert Kienfie, Angeline Khoo, and Peng Hwa Ang. 2005. "Factors Influencing Adolescents Engagement in Risky Internet Behavior." *CyberPsychology & Behavior* 8(6): 513–520.
- Lin, Holin and Chuen-Tsai Sun. 2005. "The 'White-eyed' Player Culture: Grief Play and Construction of Deviance in MMORPGs." Proceedings of *DiGRA 2005 Conference*, Vancouver: DiGRA.
- Lipsman, Andrew. 2007. "Social Networking Goes Global: Major Social Networking Sites Substantially Expanded Their Global Visitor Base during Past Year." Comscore, July 31. (<http://www.comscore.com/press/release.asp?press=1555>).

- Livingstone, Sonia and Magdalena Bober. 2004. "UK children go online: surveying the experiences of young people and their parents." London School of Economics and Political Science, July. (<http://eprints.lse.ac.uk/395/>).
- Livingstone, Sonia and Leslie Haddon. 2008. "Risky Experiences for Children Online: Charting European Research on Children and the Internet." *Children & Society* 22:314–323.
- Lo, Ven-Hwei and Ran Wei. 2005. "Exposure to Internet Pornography and Taiwanese Adolescents' Sexual Attitudes and Behavior." *Journal of Broadcasting & Electronic Media* 49(2): 221–237.
- Malamuth, Neil M. and James V. P. Check. 1981. "The Effects of Mass Media Exposure on Acceptance of Violence Against Women: A Field Experiment." *Journal of Research in Personality* 15:436–446.
- Martin, Steven P. 2003. "Is the Digital Divide Really Closing? A Critique of Inequality Measurement in a Nation Online." *IT & Society* 1(4): 1–13.
- Marwick, Alice. 2008. "To Catch a Predator? The MySpace Moral Panic." *First Monday* 13(6): article 3.
- McBride, Nancy A. 2005. "Child Safety is More Than a Slogan: "Stranger-Danger" Warning Not Effective At Keeping Kids Safer." National Missing and Exploited Children. Retrieved August 2, 2008. (http://www.missingkids.com/en_US/publications/StrangerDangerArticle.pdf).
- McKenna, Katelyn Y. A. and John A. Bargh. 2000. "Plan 9 From Cyberspace: The Implications of the Internet for Personality and Social Psychology." *Personality and Social Psychology Review* 4(1): 57–75.
- McQuade, Samuel C. and Neel M. Sampat. 2008. "Survey of Internet and At-risk Behaviors: Undertaken by School Districts of Monroe County New York." Retrieved September 13, 2008 (<http://www.rrcsei.org/RIT%20Cyber%20Survey%20Final%20Report.pdf>).
- Mehta, Michael D. 2001. "Pornography in Usenet: A Study of 9,800 Randomly Selected Images." *CyberPsychology & Behavior* 4(6): 695–703.
- Mehta, Michael D. and Dwaine E. Plaza. 1997. "Content Analysis of Pornographic Images Available on the Internet." *The Information Society* 13(2): 153–161.
- Mitchell, Kimberly, David Finkelhor, and Janis Wolak. 2005a. "Police Posing as Juveniles Online to Catch Sex Offenders: Is It Working?" *Sexual Abuse: A Journal of Research and Treatment* 17(3): 241–267.
- Mitchell, Kimberly, David Finkelhor, and Janis Wolak. 2005b. "The Internet and Family and Acquaintance Sexual Abuse." *Child Maltreatment* 10(1): 49–60.
- Mitchell, Kimberly J., David Finkelhor, and Janis Wolak. 2001. "Risk Factors for and Impact of Online Sexual Solicitation of Youth." *Journal of the American Medical Association* 285(23): 3011–3014.

- Mitchell, Kimberly J., David Finkelhor, and Janis Wolak. 2003. "The Exposure Of Youth To Unwanted Sexual Material on the Internet." *Youth & Society* 34(3): 330–358.
- Mitchell, Kimberly J., David Finkelhor, and Janis Wolak. 2004. "Emerging Issues in Child Victimization: Victimization of Youths on the Internet." *Journal of Aggression, Maltreatment, & Trauma* 8(1/2): 1–39.
- Mitchell, Kimberly J., Janis Wolak, and David Finkelhor. 2007a. "Trends in Youth Reports of Sexual Solicitations, Harassment, and Unwanted Exposure to Pornography on the Internet." *Journal of Adolescent Health* 40(2): 116–126.
- Mitchell, Kimberly J., Janis Wolak, and David Finkelhor. 2007b. "Youth Internet Users at Risk for the Most Serious Online Sexual Solicitations." *American Journal of Preventative Medicine* 32(6): 532–537.
- Mitchell, Kimberly J., Janis Wolak, and David Finkelhor. 2007c. "Online Requests for Sexual Pictures from Youth: Risk Factors and Incident Characteristics." *Journal of Adolescent Health* 41:196–203.
- Mitchell, Kimberly J., Janis Wolak, and David Finkelhor. 2008. "Are blogs putting youth at risk for online sexual solicitation or harassment?" *Child Abuse & Neglect* 32:277–294.
- Mitchell, Kimberly J. and Michele Ybarra. 2007. "Online behavior of youth who engage in self-harm provides clues for preventive intervention." *Preventative Medicine* 45:392–396.
- Mitchell, Kimberly J., Michele Ybarra, and David Finkelhor. 2007a. "The Relative Importance of Online Victimization in Understanding Depression, Delinquency, and Substance Use." *Child Maltreatment* 12(4): 314–324.
- Moessner, Chris. 2007. "Cyberbullying." Harris Interactive, April.
(http://www.harrisinteractive.com/news/newsletters/k12news/HI_TrendsTudes_2007_v06_i04.pdf).
- Murray, Craig D. and Jezz Fox. 2006. "Do Internet self-harm discussion groups alleviate or exacerbate self-harming behavior?" *Australian e-Journal for the Advancement of Mental Health* 5(3): 1–9.
- Nansel, Tonja R., Mary Overpeck, Ramani S. Pilla, Ruan W. June, Bruce Simons-Morton, and Peter Scheidt. 2001. "Bullying Behaviors Among U.S. Youth: Prevalence and Association with Psychosocial Adjustment." *Journal of the American Medical Association* 16:2094–2100.
- Nansel, Tonja R., Mary D. Overpeck, Denise L. Haynie, W. June Ruan, and Peter C. Scheidt. 2003. "Relationships Between Bullying and Violence Among U.S. Youth." *Archives of Pediatrics & Adolescent Medicine* 157(4): 348–353.
- National Center for Missing and Exploited Children. 2006. "CyberTipline Annual Report Totals."
(http://www.cybertipline.com/en_US/documents/CyberTiplineReportTotals.pdf).
- Ng, Brian D. and Peter Wiemer-Hastings. 2005. "Addiction to the Internet and Online Gaming." *CyberPsychology & Behavior* 8(2): 110–113.

- Nosko, Amanda, Eileen Wood, and Serge Desmarais. 2007. "Unsolicited online sexual material: what affects our attitudes and likelihood to search for more?" *The Canadian Journal of Human Sexuality* Spring–Summer.
- Ogilvie, Emma. 2000. "The Internet and Cyberstalking." Proceedings of *Criminal Justice Responses Conference*, Sydney: 1–7.
- Olson, Cheryl K., Lawrence A. Kutner, Dorothy E. Warner, Jason B. Almerigi, Lee Baer, Armand M. Nicholi II, and Eugene V. Beresin. 2007. "Factors Correlated with Violent Video Game Use by Adolescent Boys and Girls." *Journal of Adolescent Health* 41(1): 77–83.
- Opinion Research Corporation. 2006a. "Cyber-Bully Pre-Teen." Fight Crime: Invest in Kids, July 6. (<http://www.fightcrime.org/cyberbullying/cyberbullyingpreteen.pdf>).
- Opinion Research Corporation. 2006b. "Cyber-Bully Teen." Fight Crime: Invest in Kids, July 6. (<http://www.fightcrime.org/cyberbullying/cyberbullyingteen.pdf>).
- Palfrey, John and Urs Gasser. 2008. *Born Digital: Understanding the first generation of digital natives*. New York: Basic Books.
- Pardun, Carol J., Kelly Ladin L'Engle, and Jane D. Brown. 2005. "Linking Exposure to Outcomes: Early Adolescents' Consumption of Sexual Content in Six Media." *Mass Communication & Society* 8(2): 75–91.
- Patchin, Justin and Sameer Hinduja. 2006. "Bullies Move Beyond the Schoolyard: A Preliminary Look at Cyberbullying." *Youth Violence and Juvenile Justice* 4(2): 148–169.
- Peter, Jochen, Patti Valkenburg, and Alexander Schouten. 2005. "Characteristics and Motives of Adolescents: Talking with Strangers on the Internet and its Consequences." Presented at *International Communication Association*, New York: May 26–30.
- Peter, Jochen and Patti M. Valkenburg. 2006. "Adolescents' Exposure to Sexually Explicit Material on the Internet." *Communication Research* 33(2): 178–204.
- Pettit, Gregory S., Robert D. Laird, Kenneth A. Dodge, John E. Bates, and Michael M. Criss. 2001. "Antecedents and Behavior-problem Outcomes of Parental Monitoring and Psychological Control in Early Adolescence." *Child Development* 72(2): 583–598.
- Philips, Francesca and Gabrielle Morrissey. 2004. "Cyberstalking and Cyberpredators: A Threat to Safe Sexuality on the Internet." *Convergence: The International Journal of Research into New Media Technologies* 10(1): 66–79.
- Pierce, Tamyra A. 2006. "Talking to strangers on MySpace: Teens' use of social networking sites and the potential dangers." *Journal of Media Psychology* 11(3).
- Pierce, Tamyra A. 2007a. "Teens' Use of MySpace & The Type of Content Posted on the Sites." Retrieved July 5, 2008. (<http://www.fresno.k12.ca.us/divdept/cfen/Flyer/mySpace.pdf>).

- Pierce, Tamyra A. 2007b. "X-Posed on MySpace: A Content Analysis of 'MySpace' Social Networking Sites." *Journal of Media Psychology* 12(1).
- Ponsford, Jena. 2007. "The Future of Adolescent Female Cyber-bullying: Electronic Media's Effect on Aggressive Communication." Undergraduate Thesis, Mitte Honors Program, Texas State University.
- Ponton, Lynn E. and Samuel Judice. 2004. "Typical adolescent Sexual Development." *Child and Adolescent Psychiatric Clinics of North America* 13:497.
- Potter, Roberto H. and Lyndy A. Potter. 2001. "The Internet, Cyberporn, and Sexual Exploitation of Children: Media Moral Panics and Urban Myths for Middle-class Parents?" *Sexuality & Culture* 5(3): 31–48.
- Quayle, Ethel and Max Taylor. 2001. "Child Seduction and Self-Representation on the Internet." *CyberPsychology & Behavior* 4(5): 597–608.
- Quayle, Ethel and Max Taylor. 2002. "Child pornography and the Internet: perpetuating a cycle of abuse." *Deviant Behavior* 23(4): 331–361.
- Quayle, Ethel and Max Taylor. 2003. "Model of Problematic Internet Use in People with a Sexual Interest in Children." *CyberPsychology & Behavior* 6(1): 93–106.
- Rainie, Lee. 2005. "16% of Internet users have viewed a remote person or placing using a web cam." Pew Internet & American Life Project, June. (http://www.pewinternet.org/pdfs/PIP_webcam_use.pdf).
- Raskauskas, Juliana and Ann D. Stoltz. 2007. "Involvement in traditional and electronic bullying among adolescents." *Developmental Psychology* 43(3): 564–575.
- Rideout, Victoria. 2007. "Parents, Children & Media." Kaiser Family Foundation Survey, June. (<http://www.kff.org/entmedia/7638.cfm>).
- Rigby, Ken. 2003. "Consequences of bullying in schools." *Canadian Journal of Psychiatry* 48:583–590.
- Rimm, Martin. 1995. "Marketing Pornography on the Information Superhighway: A Survey of 917,410 Images, Descriptions, Short Stories, and Animations Downloaded 8.5 Million Times by Consumers in Over 2000 Cities in Forty Countries, Provinces, and Territories." *Georgetown Law Review* 83:1849–1934.
- Roland, Erling. 2002. "Bullying, depressive symptoms and suicidal thoughts." *Educational Research* 44:55–67.
- Rosen, Larry. 2006. "Adolescents in MySpace: Identity Formation, friendship and sexual predators." Retrieved September 9, 2008. (<http://www.csudh.edu/psych/Adolescents%20in%20MySpace%20-%20Executive%20Summary.pdf>).

- Rosen, Larry D., Nancy A. Cheever, and L. Mark Carrier. 2008. "The association of parenting style and child age with parental limit setting and adolescent MySpace behavior." *Journal of Applied Developmental Psychology* 29(6): 459–471.
- Rothenberg, Richard B. 1995. "Commentary: Sampling in Social Networks." *Connections* 18(1): 104–110.
- Sabina, Chiara, Janis Wolak, and David Finkelhor. 2008. "The Nature and Dynamics of Internet Pornography Exposure for Youth." *CyberPsychology & Behavior* 11(6): 1–3.
- Salter, Anna. 2004. *Predators: Pedophiles, Rapists, and Other Sex Offenders*. Cambridge, MA: Basic Books.
- Schiano, Diane J., Coreena P. Chen, Jeremy Ginsberg, Unnur Gretarsdottir, Megan Huddleston, and Ellen Isaacs. 2002. "Teen Use of Messaging Media." Proceedings of *CHI*, Minneapolis, Minnesota.
- Seals, Dorothy and Jerry Young. 2003. "Bullying and victimization: Prevalence and relationship to gender, grade level, ethnicity, self-esteem and depression." *Adolescence* 38:735–747.
- Seay, A. Fleming and Robert E. Kraut. 2007. "Project Massive: Self-Regulation and Problematic Use of Online Gaming." Proceedings of *SIGCHI*, San Jose, CA: 829–838.
- Seto, Michael C., James M. Cantor, and Ray Blanchard. 2006. "Child Pornography Offenses Are a Valid Diagnostic Indicator of Pedophilia." *Journal of Abnormal Psychology* 115(3): 610–615.
- Shade, Leslie Regan. 2003. "Weborexics: The Ethical Issues Surrounding Pro-Ana Websites." Proceedings of *ACM SIGCAS Computers and Society*, Boston: ACM, 107–116.
- Shadish, William R., Thomas D. Cook, and Donald T. Campbell. 2001. *Experimental and Quasi-Experimental Designs for Generalized Causal Inference*. Boston, MA: Houghton Mifflin Company.
- Sheldon, Kerry and Dennis Howitt. 2007. *Sex Offenders and the Internet*. West Sussex, England: Wiley.
- Sheridan, Lorraine P. and T. Grant. 2007. "Is Cyberstalking Different?" *Psychology, Crime & Law* 13(6): 627–640.
- Skinner, Carrie-Ann. 2008. "20% of UK Kids Meet Facebook 'Friends'." (http://www.pcworld.com/article/149636/20_of_uk_kids_meet_facebook_friends.html).
- Slonje, Robert and Peter K. Smith. 2008. "Cyberbullying: Another main type of bullying?" *Scandinavian Journal of Psychology* 49: 147–154.
- Šmahel, David and Kaveri Subrahmanyam. 2007. "Any Girls Want to Chat Press 911: Partner Selection in Monitored and Unmonitored Teen Chat Rooms." *CyberPsychology & Behavior* 10(3): 346–353.
- Smith, Aaron. 2007. "Teens and Online Stranger Contact." Pew Internet & American Life Project, October 14. (http://www.pewinternet.org/PPF/r/223/report_display.asp).
- Smith, Anita and Kipling D. Williams. 2004. "R U There? Ostracism by Cell Phone Text Messages." *Group Dynamics: Theory, Research, and Practice* 8(4): 291–301.

- Smith, Peter K., Jess Mahdavi, Manuel Carvalho, Sonja Fisher, Shanette Russell, and Neil Tippett. 2008. "Cyberbullying: its nature and impact in secondary school pupils." *Journal of Child Psychology and Psychiatry* 49(4): 376–385.
- Snyder, Howard N. and Melissa Sickmund. 2006. "Juvenile Offenders and Victims: 2006 National Report." U.S. Department of Justice, March. (<http://ojjdp.ncjrs.gov/ojstatbb/nr2006/index.html>).
- Soukup, Charles. 2000. "Building a Theory of Multimedia CMC." *New Media & Society* 2(4): 407–425.
- Southern Poverty Law Center. 2004. "Hate Groups, Militias on Rise as Extremists Stage Comeback." (<http://www.splcenter.org/center/splcreport/article.jsp?aid=71>).
- Stahl, Christiane and Nancy Fritz. 1999. "Internet Safety: Adolescents' Self-report." *Journal of Adolescent Health* 31:7–10.
- Steinberg, Laurence and Jennifer S. Silk. 2002. "Parenting adolescents." In *Handbook of parenting: Volume 1. Children and parenting*, edited by M. H. Bornstein, 103-134. Mahwah, NJ: Erlbaum.
- Stys, Yvonne. 2004. "Beyond the Schoolyard: Examining Bullying Among Canadian Youth." Carleton University.
- Subrahmanyam, Kaveri and Patricia Greenfield. 2008. "Online Communication and Adolescent Relationships." *The Future of Children* 18(1): 119–146.
- Sue, Valerie M. and Lois A. Ritter. 2007. *Conducting Online Surveys*. Thousand Oaks, CA: Sage.
- Taylor, Max and Ethel Quayle. 2003. *Child Pornography—An Internet Crime*. East Sussex, UK: Brunner-Routledge.
- Thelwall, Mike. 2008. "Social networks, gender, and friending: An analysis of MySpace member profiles." *Journal of the American Society for Information Science and Technology* 59(8): 1523–1527.
- Thomas, Jim. 1996. "When Cyberresearch Goes Awry: The Ethics of the Rimm "Cyberporn" Study." *The Information Society* 12(2): 189–198.
- Thompson, Kimberly M. and Kevin Haninger. 2001. "Violence in E-Rated Video Games." *Journal of the American Medical Association* 286(5): 591–598.
- Thompson, Kimberly M., Karen Tepichin, and Kevin Haninger. 2006. "Content and Rating of Mature-Rated Video Games." *Archives of Pediatrics & Adolescent Medicine* 160(4): 402–410.
- Tynes, Brendesha, Lindsay Reynolds, and Patricia M. Greenfield. 2004. "Adolescence, race, and ethnicity on the Internet: A comparison of discourse in monitored vs. unmonitored chat rooms." *Journal of Applied Developmental Psychology* 25:667–684.
- Valentine, Gill. 2004. *Public Space and the Culture of Childhood*. Hants, England: Ashgate.
- van Dijk, Jan and Kenneth Hacker. 2003. "The Digital Divide as a Complex and Dynamic Phenomenon." *The Information Society* 19(4): 315–326.

- Walther, Joseph B., Celeste L. Slovacek, and Lisa C. Tidwell. 2001. "Is a Picture Worth a Thousand Words? Photographic Images in Long-term and Short-Term Computer-Mediated Communication." *Communication Research* 28(1): 105–134.
- Warner, Dorothy E. and Mike Ratier. 2005. "Social Context in Massively-Multiplayer Online Games (MMOGs): Ethical Questions in Shared Space." *International Review of Information Ethics* 4:7.
- Webb, Liane, Jackie Craissati, and Sarah Keen. 2007. "Characteristics of Internet Child Pornography Offenders: A Comparison with Child Molesters." *Sexual Abuse* 19(4): 449–465.
- White, Leneigh, Carol Gregory, and Christine Eith. 2008. "The Impact of Accidental Exposure to Cyberpornography on Sexual Offending Among Youth: A Case Study." Proceedings of *The annual meeting of the American Society of Criminology*, Royal York, Toronto.
- Whitlock, Janis L., Jane L. Powers, and John Eckenrode. 2006. "The Virtual Cutting Edge: The Internet and Adolescent Self-Injury." *Developmental Psychology* 42(3): 407–417.
- Williams, Dmitri and Marko Skoric. 2005. "Internet Fantasy Violence: A Test of Aggression in an Online Game." *Communication Monographs* 72(2): 217–233.
- Williams, Dmitri, Nick Yee, and Scott E. Caplan. 2008. "Who plays, how much, and why? Debunking the stereotypical gamer profile." *Journal of Computer Mediated Communication* 13:993–1018.
- Williams, Kirk R. and Nancy G. Guerra. 2007. "Prevalence and Predictors of Internet Bullying." *Journal of Adolescent Health* 41:S14–S21.
- Wolak, Janis, David Finkelhor, and Kimberly Mitchell. 2005. "The Varieties of Child Porn Production." In *Viewing child pornography on the Internet: Understanding the offense, managing the offender, helping the victims*, edited by E. Quayle & M. Taylor, 31–48. Dorset, UK: Russell House Publishing.
- Wolak, Janis, David Finkelhor, and Kimberly Mitchell. 2008a. "Is Talking Online to Unknown People Always Risky? Distinguishing Online Interaction Styles in a National Sample of Youth Internet Users." *CyberPsychology & Behavior* 11(3): 340–343.
- Wolak, Janis, David Finkelhor, Kimberly Mitchell, and Michele Ybarra. 2008b. "Online "Predators" and Their Victims: Myths, Realities, and Implications for Prevention and Treatment." *American Psychologist* 63(2): 111-128.
- Wolak, Janis, David Finkelhor, and Kimberly J. Mitchell. 2004. "Internet-initiated Sex Crimes against Minors: Implications for Prevention Based on Findings from a National Study." *Journal of Adolescent Health* 35(5): 424.e11–424.e20.
- Wolak, Janis, Kimberly J. Mitchell, and David Finkelhor. 2002. "Close Online Relationships in a National Sample of Adolescents." *Adolescence* 37(147): 441–455.

- Wolak, Janis, Kimberly J. Mitchell, and David Finkelhor. 2003a. "Escaping or connecting? Characteristics of youth who form close online relationships." *Journal of Adolescence* 26:105–119.
- Wolak, Janis, Kimberly J. Mitchell, and David Finkelhor. 2003b. "Internet Sex Crimes Against Minors: The Response of Law Enforcement." National Center for Missing and Exploited Children, November. (<http://www.unh.edu/ccrc/pdf/CV70.pdf>).
- Wolak, Janis, Kimberly Mitchell, and David Finkelhor. 2006. "Online Victimization of Youth: Five Years Later." National Center for Missing and Exploited Children, #07-06-025. (<http://www.unh.edu/ccrc/pdf/CV138.pdf>).
- Wolak, Janis, Kimberly J. Mitchell, and David Finkelhor. 2007a. "Does Online Harassment Constitute Bullying? An Exploration of Online Harassment by Known Peers and Online-Only Contacts." *Journal of Adolescent Health* 41:S51–S58.
- Wolak, Janis, Kimberly J. Mitchell, and David Finkelhor. 2007b. "Unwanted and Wanted Exposure to Online Pornography in a National Sample of Youth Internet Users." *Pediatrics* 119(2): 247–257.
- Wolak, Janis, Michele Ybarra, Kimberly J. Mitchell, and David Finkelhor. 2007c. "Current Research Knowledge About Adolescent Victimization on the Internet." *Adolescent Medicine* 18:325–241.
- Wolfe, David A. and Debbie Chiodo. 2008. "Sexual Harassment and Related Behaviors Reported Among Youth from Grade 9 to Grade 11." CAMH Centre for Prevention Science, February 5. (http://www.camh.net/News_events/Media_centre/CAMH%20harassment%20paper.pdf).
- World Health Organization. 2007. "International Statistical Classification of Diseases and Related Health Problems, 10th Revision." (<http://www.who.int/classifications/apps/icd/icd10online/>).
- Ybarra, Michele. 2004. "Linkages between Depressive Symptomology and Internet Harassment among Young Regular Internet Users." *CyberPsychology & Behavior* 7(2): 247–257.
- Ybarra, Michele, Cheryl Alexander, and Kimberly J. Mitchell. 2005. "Depressive symptomatology, youth Internet use, and online interactions: A national survey." *Journal of Adolescent Health* 36(1): 9–18.
- Ybarra, Michele, Marie Diener-West, and Philip J. Leaf. 2007a. "Examining the Overlap in Internet Harassment and School Bullying: Implications for School Intervention." *Journal of Adolescent Health* 41:S42–S50.
- Ybarra, Michele, Dorothy L. Espelage, and Kimberly J. Mitchell. 2007b. "The Co-occurrence of Internet Harassment and Unwanted Sexual Solicitation Victimization and Perpetration: Associations with Psychosocial Indicators." *Journal of Adolescent Health* 41:S31–S41.
- Ybarra, Michele, Philip J. Leaf, and Marie Diener-West. 2004. "Sex Differences in Youth-Reported Depressive Symptomatology and Unwanted Internet Sexual Solicitation." *Journal of Medical Internet Research* 6(1).

- Ybarra, Michele, Kimberly Mitchell, David Finkelhor, and Janis Wolak. 2007. "Internet Prevention Messages: Targeting the Right Online Behaviors." *Archives of Pediatrics & Adolescent Medicine* 161:138–145.
- Ybarra, Michele, Kimberly Mitchell, Janis Wolak, and David Finkelhor. 2006. "Examining Characteristics and Associated Distress Related to Internet Harassment: Findings from the Second Youth Internet Safety Survey." *Pediatrics* 118(4): e1169–e1177.
- Ybarra, Michele and Kimberly J. Mitchell. 2004a. "Online aggressor/targets, aggressors, and targets: a comparison of associated youth characteristics." *Journal of Child Psychology and Psychiatry* 45(7): 1308–1316.
- Ybarra, Michele and Kimberly J. Mitchell. 2004b. "Youth engaging in online harassment: associations with caregiver-child relationships, Internet use, and personal characteristics." *Journal of Adolescence* 27:319–336.
- Ybarra, Michele and Kimberly J. Mitchell. 2005. "Exposure to Internet Pornography among Children and Adolescents: A National Survey." *CyberPsychology & Behavior* 8(5): 473–486.
- Ybarra, Michele and Kimberly J. Mitchell. 2007. "Prevalence and Frequency of Internet Harassment Instigation: Implications for Adolescent Health." *Journal of Adolescent Health* 41:189–195.
- Ybarra, Michele and Kimberly J. Mitchell. 2008. "How Risky Are Social Networking Sites? A Comparison of Places Online Where Youth Sexual Solicitation and Harassment Occurs." *Pediatrics* 121(2): e350–e357.
- Yee, Nick. 2006. "The Demographics, Motivations, and Derived Experiences of Users of Massively Multi-User Online Graphical Environments." *Presence* 15(3): 309–329.
- Zhou, Yilu, Edna Reid, Jialun Qin, Hsinchun Chen, and Guanpi Lai. 2005. "U.S. Domestic Extremist Groups on the Web: Link and Content Analysis." *IEEE Intelligent Systems* 20(5): 44–51.

APPENDIX D:
Technology Advisory Board Report

EXECUTIVE SUMMARY

The Technology Advisory Board (TAB) solicited, evaluated, reviewed, 40 written submissions of technologies and drew conclusions from these submissions about the state of online safety technology for minors in a formal process described in detail in this document. The primary task was to assess whether and how the submitted technologies could be useful in the context of enhancing online safety for minors.

In sum, the TAB review of the submitted technologies leaves us in a state of cautious optimism, with many submissions showing promise. The children's online safety industry is evolving, and many of the technologies we reviewed were point solutions rather than broad attempts to address the children's safety 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. Thus, 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 ultimately 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. But clearly there is a role for technology in addressing this issue both now and in the future, and most likely, various technologies could be leveraged together to 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 although 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. Likewise, education is an essential part of the puzzle. Even the best technology or technologies should be only part of a broader solution to keeping minors safer online.

As a corollary, the TAB also recommends that further evaluative work be conducted on any technology – whether or not it was among those reviewed in this process – prior to broadly recommending its use, given the potential for new risks and significant unintended consequences. The benefits of each reviewed solution 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 also not 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 later in this document, are the specific conclusions and recommendations generated by the TAB's review process:

- ***Technology can play a role but cannot be the sole input to improved safety for minors online.***
- ***The most effective technology solution is likely to be 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.***

INTRODUCTION

The scope of the Technology Advisory Board's mandate in conducting its work for the Task Force was to review all submissions that it received detailing technology solutions for improved online safety for minors. To conduct its work, the TAB was limited to the written 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.

Based on these inputs, we discuss broad sets of technology categories that address several online safety concerns involving minors. For each category, we summarize how the technologies address one or more aspects of online safety for minors, the potential benefits of the approach, and hurdles that it must overcome to be effective.

PROCESS AND METHODOLOGY

Technology Advisory Board Members and Observers

The Technology Advisory Board comprised two teams: the TAB Members and the TAB Observers. The TAB Members team was charged with the formal review of the technology submissions from third parties. The TAB Observers team was asked to formally comment on any or all of the submissions if they so chose, but, due to potential conflicts of interest, their comments were neither part of the formal technology reviews nor part of the recommendation process to select presenters for the Berkman ISTTF Public Meeting.

The objective in building the TAB teams was to enlist people who had deep technology backgrounds, domain expertise in a field related to the Task Force's work, and a demonstrated professional interest in relevant subject areas. In addition to technology professionals, we also added representatives from other related fields to serve as Observers, so that we could draw on their areas of expertise. An additional distinction between Members and Observers is that Observers might have conflicts of interest with the review work.

Nominations for both Members and Observers came from the Task Force itself, the Task Force team at the Berkman Center, other Berkman Center affiliates, and other TAB Members and Observers. The nominations were vetted through the Berkman Task Force team, an interview and investigation of possible conflicts of interest were conducted, and then the Berkman Task Force team made the decision whether to invite the nominee to join the TAB Members or Observers team.

TAB Members (Complete biographies are included as Exhibit 1)

Ben Adida, Harvard Medical School, Harvard University

Scott Bradner, Harvard University

Laura DeBonis, Berkman Center, Harvard University

Hany Farid, Dartmouth

Lee Hollaar, University of Utah

Todd Inskeep, Bank of America
Brian Levine, University of Massachusetts Amherst
Adi Mcabian, Twistbox
RL Morgan, University of Washington
Lam Nguyen, Stroz Friedberg, LLC
Jeff Schiller, MIT
Danny Weitzner, MIT

TAB Observers (Complete biographies are included as Exhibit 1)

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

Soliciting, collecting, and evaluating submissions

Soliciting

The process for soliciting submissions was as follows: the TAB created a Submission Template that encompassed the various questions anticipated for any single technology. Primary areas for response included: (1) functional goals that a technology attempted to address; (2) technological detail about the technology itself; and (3) financial and other business information about the technology to inform the assessment of viability and functionality. On July 1, 2008, the Submission Template was posted to the Task Force's webpage on the Berkman website and made broadly available for download by any company, individual, or other entity that wished to submit, in writing only, a technology for consideration. (The Submission Template is included as Exhibit 2.)

The public was made aware of the Template through a Berkman Center press release and by tapping into various networks, including networks of the Berkman Center staff and affiliates, the TAB, and the members of the Task Force.

The deadline for submission was July 21, 2008, approximately three weeks after the Template was made publicly available.

Collecting

In total, the TAB received 40 written submissions from 38 companies. (An additional submission involving a registry for minors' email addresses was withdrawn from consideration by the submitting company.) Submitters were asked to include with their submission a statement indicating that they understood the Intellectual Property policy regarding submission to the Task Force. (The Intellectual Property policy is included as Exhibit 3.)

Evaluating

The TAB designed and the Berkman Task Force team approved an evaluation process that closely followed the model of other scientific reviews; in particular, that of the National Science Foundation review. Three to five TAB Members reviewed each document. Following initial discussions of the document, questions were sent to the submitting companies to clarify our understanding of their submission. All companies responded to the follow-up questions. Final review discussions considered the answers to the follow-up questions as well as all TAB Observer Comments. After final review discussions, recommendations were made to the Berkman Task Force team for companies to present at the Public Meeting of the Task Force. Many criteria were involved in determining whether a submitting company was asked to present at the Public Meeting. A recommendation to have a company present was not an endorsement of the technology. Rather, the TAB sought to have a variety of technologies, companies, and approaches discussed; to show the range of ideas extant; to inform the public; and to help foster meaningful dialogue about solutions to improving online safety for minors.

Evaluation questions were circulated to the Members of the TAB prior to their initial reading of the submissions. Members were asked to use the questions to frame their thinking in preparation for review discussions. The evaluation questions included:

- What functional requirements are met by the submission?
- What is the overall approach?
- Who is the target audience (e.g., youth under 13, teens, parents)?
- What is the target system (e.g., social networking sites, cell phones, ISPs)?
- What underlying assumptions does the proposal make? Are they reasonable?
- Does the approach require education and/or parental involvement?
- What are the strengths and weakness of the approach?
- How well does the product actually address its targeted function?
- What are unintended consequences caused by use of the product?
- Under what circumstances would the product fail? How often?
- What are the consequences of product failure?
- What other trade-offs does the product present?
- How does product work internationally?
- How does product work with different business models?

To facilitate the review process, the TAB created a list of functional goals related to online safety for minors that a technology might address. This list was included as one of the sections in the Submission Template and each company self-identified one or more of eight functional goals for the technology. For the purposes of review, the different solutions submitted were clustered according to these functional goals:

- Limit harmful contact between adults and minors
- Limit harmful contact between minors
- Limit/prevent minors from accessing inappropriate content on the Internet

- Limit/prevent minors from creating inappropriate content on the Internet
- Limit the availability of illegal content on the Internet
- Prevent minors from accessing particular sites without parental consent
- Prevent harassment, unwanted solicitation, and bullying of minors on the Internet
- Other – please specify

In addition to self-identification of functional goals, after review, the TAB also assigned one of five categories to each of the 40 technology submissions. Occasionally more than one category applied to a technology; in such situations, the primary category was the one with which the technology was associated.

The technology categories, with number of submissions received in parentheses, are:

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

A list of all submissions in alphabetical order is included as Exhibit 4. The submissions themselves as well as TAB Observer Comments are available on the Task Force's website.

ANALYSIS

Among past efforts to survey the landscape of children's online safety technologies, the 2000 COPA Commission report is one of the most relevant. For purposes of brevity we do not summarize or cite COPA or other previous reviews of technologies in our analyses below. The TAB does recognize, however, the importance of previous work in this area. Our intention with this review process is to complement previous work and not to supersede it.

Below we summarize the categories of technology solutions presented, comment occasionally on particular technologies, and discuss overall the strengths and weaknesses of each category in application to enhancing online safety for minors. In each category, some solutions help a little bit and some help more extensively. The same is true of each category of technology. We considered each proposal from the perspective of what the potential outcome would be if it were fully implemented and widely adopted. Again, no one solution can solve the entire youth online safety problem, but it was clear from the submissions that there has been excellent traction achieved.

Age Verification/Identity Authentication

Category Description

Age verification technologies seek primarily to verify the age of adults and children, while identity technologies seek to verify individual identities. The primary goal of these technologies is to utilize age as a mechanism for limiting inappropriate contact between children and adults as well as preventing access by minors to inappropriate content. Although some technologies attempt to verify age/identity remotely, other technologies rely on a trusted third party for verification (e.g., schools, notaries, or government agencies). A submission in this category involving a registry of minors' email addresses was withdrawn from consideration by the submitting company.

We separated technology submissions in this area into four subcategories:

1. Comparison against records collected from public databases. Many records, both public and private, are available about adults, including information from credit reports, criminal history, and real estate transfers. These disparate records can be aggregated into a portfolio of data about an individual. This information can then be used, among other applications, as a basis to present challenge questions to individuals to ensure their correct identification.
2. Comparison against records collected by schools or other public entities. Records about children are difficult for third parties to collect. This subcategory of submissions commonly relies on schools or other public entities (e.g., a post office or DMV) to verify the age of a child through a designee. Permission of the parents/child is required for initial access to and use of these records.
3. Peer-based verification, which allows peers in a community to vote, recommend, or rate whether a person is in an appropriate age group based on relationships and personal knowledge established offline.
4. Biometrics. Biometric solutions involve using an individual's inherent characteristics, such as physiological traits or facial images, to verify age. These solutions are discussed in the biometrics section of this document.

Commentary

- In general, some submissions attempt to make it more difficult for minors to pretend to be adults, while others focus on making it more difficult for adults to pretend to be minors. Rarely does one technology address both problems.
- Typically, these technologies do make it more difficult for a minor to pose as an adult to whom they are not related or acquainted. Similarly, they also typically make it harder for an adult to pose as a minor who is not a family member or is otherwise unknown to them.

- Many of these technologies are designed primarily for the United States context and may not functionally optimally in international contexts.
- Peer-based methods suffer from the same basic limitation seen in many an online poll or online peer-rated merchant sites: users can vote as many times as they wish to artificially raise or lower a peer rating. Additionally, if left unchecked, users can even create multiple identities to perform the extra voting themselves. Finally, even if all identities in the system are real and unique, minors might organize against another minor in their ratings or recommendations in an online form of bullying increasingly known as cyberbullying.
- Comparison against public records is only as effective as the completeness and data quality of the public database. This approach is more suitable to verifying the age of adults as public records of minors range from quite limited to nonexistent. There are also significant privacy concerns when institutions that hold the records of minors (e.g., schools) are involved.
- The public entity–based approach, though appealing in terms of the accuracy of its data, has significant challenges from a practical perspective. Resources, incentives, legal liability and basic infrastructure are each nontrivial potential hurdles to achieving scale with this solution. For example, the coordination and participation of thousands of public entities (often resource-constrained already) would be a significant operational challenge on the aggregator side.
- More generally, in all of these approaches, the user receives digital credentials after verification that can be used across sessions without reverifying. These credentials, which are usually protected by only a user name and password, are easy to transfer from adult to child or from child to adult. Further, they can be sold, traded cooperatively, or taken under duress.
- The working assumption for technologies in this category is that age- or identity-related deception is at the center of sexual solicitation on the Internet. Some emerging research, such as that documented by the Task Force's Research Advisory Board, suggests that this may not be the central issue in online sexual solicitation. Thus, although these types of solutions do target potential risks, they may not target the most critical issues that underlie Internet-based sexual solicitation.
- Finally, there are significant potential privacy concerns and security issues given the type and amount of data aggregated and collected by the technology solutions in this category, each needing to be thoughtfully addressed and well-managed.

Conclusion

Age verification and identity authentication technologies are appealing in concept but challenged in terms of effectiveness. Any system that relies on remote verification of information has potential for inaccuracies. For example, on the user side, it is never certain that the person attempting to verify an identity is using their own actual identity or someone else's. Any system that relies on public records has a better likelihood of accurately verifying an adult than a minor due to extant records. Any system that focuses on third-party in-person verification would require significant political backing and social acceptance. Additionally, any central repository of this type of personal information would raise significant privacy concerns and security issues.

Filtering/Monitoring/Auditing

Category Description

Filtering, monitoring and auditing solutions attempt either to prevent a user from accessing inappropriate content or provide a monitoring mechanism to document this activity after it occurs. These tools are based on a set of predetermined criteria that allow dynamic monitoring of web content and on-the-fly determination of the appropriate level of access. They are usually software-based and installed on a user's computer. They can often be packaged with logging features that allow an individual to review prior Internet activity on the computer. Historically, filtering, monitoring, and auditing tools have enjoyed widespread success and have been in use by parents, schools, and other public venues in which Internet restrictions are appropriate.

Filtering, monitoring, and auditing tools are generally divided into two categories: client-side and server-side.

- Client-side software is installed locally on the user's computer and is maintained by the user. Its effectiveness is dependent on the user's installation, configuration, regular maintenance, and use of the software. Client-side filtering tools are very popular and have been deployed for over a decade. They are relatively straightforward to implement and offer parents and guardians an easy way to provide a safer Internet environment.
- In the server-side approaches reviewed by the TAB, filtering of inappropriate content is performed before the content reaches a user's computer and is bounded by the standards of the website or service platform itself. (As a note, "server-side filtering" is often used to refer to content filtering at the ISP level. The TAB received no submissions for ISP-level filtering products.) For example, a social network site can filter – or flag – user-generated content that is deemed inappropriate for some users. Thus, a website's policy, rather than individual user's preferences, dictates the level of appropriateness, with the scope limited to just that site.

Commentary

- Client-side filtering can be effective as a complementary solution to other technologies, is readily deployable by a parent or responsible adult, and is reasonably easy to use. A possible downside of client-side filtering may be that it might provide users with the illusion of total safety and problem prevention and thereby reduce critical adult vigilance and involvement. Additionally, costs may prevent families from choosing this option.
- The effectiveness of a filtering tool may vary based on its design and amount of user control. Some filters do analysis on the fly, and some filters are based on a predetermined set of criteria. For this latter group, their restrictions vary greatly based on the software manufacturer. Overly restrictive tools can filter out too much information, leaving its users frustrated and resulting in a reversion to less restrictive settings, and thereby exposure to greater risk.
- Some filtering tools address all Internet technologies, but some do not. For example, one package can restrict access to inappropriate websites but still allow unfiltered conversations to occur over instant messaging programs. Finally, although many programs offer users a varying degree of control over what they filter, frequently filtering software makes decisions that rely on its own criteria, not that of the parents, limiting parents' control over what they deem appropriate.
- Commonly, these filters can detect certain types of inappropriate content, but the focus of filtering software is more on prevention of access to pornographic content than it is to violent images and video or content involving self-harm. These tools also function more accurately with text and images than with video and audio. For continued effectiveness, it is critical that filtering tools must constantly adapt to the constant changes in Internet technologies.
- Though relatively easy to implement, filtering tools typically require a software purchase and enough technological ability to install the application. Additionally, they require the time and understanding to properly configure the software for the appropriate age level and often require regular updates via the Internet. The issue here is that responsible adults may not be computer-literate enough to be comfortable with installation, configuration, and updates, which may ultimately put minors at risk.
- Filtering software can be easily circumvented or disabled by computer-savvy users, completely eliminating their effectiveness. Frequently, parents or guardians are notified in such cases, which is beneficial. In any case, parents, guardians, and other caregivers should simply be alert to the potential for circumvention.
- Server-side filtering, though appealing for its ease of use, presents concerns about potential lack of parental control over access to content and also, at the extreme, about potential censorship.

- Auditing software typically requires regular commitment from parents or other responsible adults for effectiveness. The benefit and the challenge of auditing software is the potentially vast amount of data captured about a minor's online activity. This data, however, requires some sort of adult review, commonly available in summary fashion, for actual efficacy. There is limited impact on online safety for minors from using auditing software without the ongoing attention of a responsible adult.
- To make auditing more manageable, monitoring software often stores activity logs in a central location owned by the software provider. These records are therefore potentially at risk for compromise by hackers, have the potential to be sold to third parties seeking marketing data, and have other privacy and security issues as well.

Conclusion

Filtering, monitoring and auditing software can provide parents and other supervisory adults with a useful tool to assist in determining and limiting user access to certain types of inappropriate Internet content. Although not a total solution for minors' online safety, the effective use of these types of tools can be a key part of a holistic solution whereby parental involvement, adult supervision, and software tools work together to provide a safer Internet environment.

Text Analysis

Category Description

Text-based analysis technologies are designed to automatically detect predatory, harassing, or otherwise inappropriate conversations on the Internet. These solutions generally work by obtaining samples of the conversations to be detected, extracting a statistical signature from these conversations, and classifying them based on the measured statistic. Text analysis tools vary in their deployment schemes, ranging from local installation at Internet cafes, libraries, and other public access sites to large-scale deployments across an entire social network website. Some solutions even incorporate the automated analysis as part of a parental auditing tool, locally operating on a home computer.

Commentary

- Automated text analysis can be quite useful against inappropriate interactions including online harassment, sexual solicitation, and other types of problematic communications, as it primarily focuses on language and highlights potential problems early.
- Given the sheer volume of online interactions and communications, the development of automated techniques for analyzing text conversations seems

quite reasonable. To be effective, however, it is crucial that a statistically valid sample of representative text be collected to use as a baseline. There are two challenges to this sampling effort: millions of text-based messages are exchanged across the Internet every day, so not only does obtaining a valid “going forward” sample present a challenge, but retrospectively acquiring and tracking data to adequately identify an escalating situation would also be complicated.

- An area for further development for text analysis technologies is error rate. The current typical error rate in analyzing contextual text is problematic. Not enough research has been done yet to determine the impact of known error rates. It is likely that any large-scale implementation of text analysis technology would produce far too many false positives at this point in time, and would require additional, non-scalable manual effort to identify illicit behavior. An additional risk is that legitimate users may be denied access to Internet-based services that automatically blacklist users based on criteria. The problem also exists in the reverse. A low rate of positive identification can minimize the dangers posed on the Internet, provide a false sense of security, and actually endanger the individuals it intends to protect.
- International environments such as the Internet also present challenges to automated text analysis technology. The proposed solutions currently seemed unlikely to scale to encompass the wide variety of languages, colloquial dialects, and conversational styles present on the Internet and probably essential over time to effective text analysis. Effective systems must also evolve to take into account the various ways in which users try to circumvent the filters by altering their linguistic patterns.
- The automated text analysis technologies submitted presented some potential privacy and security concerns, particularly in the cases in which a tool proposed to track and store historical data on its servers. Internet users would be unwittingly subjected to intrusions on what may be legitimate and private conversations.

Conclusion

Text analysis technologies overall seemed to be a promising category of technology solution for improving online safety for minors, but the slate of submissions in this category were in a relatively early stage of development at this time. To accommodate for current shortcomings, certain implementations of automated text analysis could still be effective. Situations in which a parent uses the technology as a complement to other filtering, monitoring, and auditing activities may assist in the supervision of a child on the Internet. Schools and other public institutions that provide clear notice to its users, deploy the tool locally as part of an overall security program, and use consistent standards to manually review the text after identification may also find it useful. Lastly, websites that deploy the solution as part of an active monitoring and supervision program may find it assists in reducing the need for manual oversight. Although these benefits may outweigh

possible concerns, it is incumbent on an entity to thoroughly test and understand the limitations of the tool prior to its deployment and, overall, the TAB felt that text analysis tools needed to evolve a bit further prior to widespread deployment and usage.

Biometrics

Category Description

Biometric technologies attempt to identify an individual or class of individuals based upon intrinsic physical (e.g., fingerprint, iris, or DNA) or behavioral traits (e.g., walking gate or typing style). Significant research has gone into the development of biometric technologies and some have been deployed in limited commercial settings.

These tools often use a hardware-based device to accept and transmit certain biometric information through the computer. In one instance, a device attempts to determine an individual's age grouping based on a bone density analysis of that individual's hand. Another tool attempts to actually identify a specific individual through facial recognition and match the individual to a known sex offender database. Others are still more novel in their approach, attempting to identify specific individuals through the analysis of a user's typing behavior and patterns.

In each instance, information is gathered by either the hardware or software tool and submitted to determine the appropriateness of an individual using a particular service. The website or web service employing this solution incorporates the safeguard in their system and where necessary, requires the user to purchase the biometric device for their computer.

Commentary

- In limited situations, biometric techniques may provide a solution to assisting in limiting inappropriate contact between adults and minors. These solutions, however, are challenged with problems that can undermine their usefulness in addition to being expensive to deploy.
- Biometric solutions typically require supervision to be effective. A situation in which individuals are expected to self-identify through the use of a biometric device over the Internet is, at best, suboptimal. Individuals can obfuscate a facial image through the use of varied lighting, facial hair, and other indistinguishable features. Typing styles and patterns can vary drastically depending on the type of keyboard, the use of voice-recognition software, and an almost unlimited number of variables from computer to computer. Bad actors can use their own children or other individuals to submit false readings. The challenges to positive, accurate identification are numerous, especially in Internet-based deployments in which an individual is not monitored while using their biometric device.
- Accuracy rates are critical for effectiveness. The level of accuracy in the submitted tools has not yet been proven and could be problematic, resulting in

potential denial of access for legitimate users to a particular website or web service.

- The working assumption of biometric technologies is that identity deception is at the root of online safety problems. Although this may be true in some percentage of cases, the research documented by the Task Force's Research Advisory Board suggests that deception is not the central issue in online safety for minors.
- Any biometric system raises important privacy concerns and security issues, particularly if the biometric data is transmitted or stored on a central server, presenting challenges to both user and business adoption. Biometric data is, by law, considered Personally Identifying Information (PII). Servers holding large amounts of PII pose a serious security risk and would be a likely target for information theft. The retention and security of this data would present a significant business liability and might have a deterrent effect on potential users. It is possible that business risk alone would likely deter any wide scale adoption, without legislation or mandate.

Conclusion

Biometric solutions certainly have some appeal, if proven effective, and show some promise, should they continue to evolve. At present, however, there are significant challenges to widespread usage and adoption for a variety of reasons including accuracy and detection rates and a need for supervision.

Other: Individual Identification

Category Description

Submissions in the category focused on identifying or profiling individuals who have been convicted of sex offenses, for example by aggregating data from registered sex offender databases or by tracking devices and computers of registered sex offenders. These technologies then enable a website to block or otherwise prevent the individuals profiled from accessing a site or areas on a site.

Commentary

- Profiling systems are only as effective as the data they use. Not all potential problem users have been previously identified or registered in the sex offender database or other watchlists; thus, a system relying on such data will be inherently limited.
- Basing a technology solution on user-provided information is a challenge to the accuracy of any technology. It is not clear that adequate incentive exists for a user to provide accurate information in this context. Further, acquiring and using invalid personal information is a trivial exercise.

- Solutions that require a computer to be used by a single user only for effectiveness will have limited deployment options and limited effectiveness in a world where public computers with Internet access are fairly widely available. Libraries, schools, and even households can have many users that may have completely different intentions.
- Identification systems require high accuracy rates for effectiveness and adoption. Problematic accuracy rates may result in legitimate users potentially being denied access to a particular web site or service. For example, a user who shares a name or identifying information with someone in a Registered Sex Offender database might be inappropriately denied access.
- With the use of personal information essential to the functioning of many of these systems, robust data privacy and security policies and technology are critical to their success.

Conclusion

These profiling technologies represent very specific point solutions, each with its particular challenges to effectiveness but also with potentially positive benefits to usage. Should accuracy issues be addressed, these types of technologies could probably be deployed in concert with other complementary technologies to improve online safety concerns for minors.

CASE STUDY: icouldbe.org

Although icouldbe.org did not propose an explicit technology solution, but rather a general description of their enterprise, they presented a complete approach to ensuring safe interactions between teenagers and adults in their secure online community. Specifically, icouldbe.org pairs underserved teenage students with adult mentors who aid students in career development, education planning, and general mentoring. All student/mentor interactions occur online, and icouldbe.org goes to great efforts to ensure that students and mentors do not interact outside of their website or have any type of personal or physical contact. To do so, icouldbe.org has implemented a number of complementary technologies, achieving what appears to be – so far, at least – a successful and effective secure community. These technologies include text-based filtering to make sure that email addresses, personal URLs, telephone numbers, or other personal identifying information are not included in any correspondence between the mentee and mentor. Additionally, icouldbe.org does extensive verification and background searches on all mentors to allow only appropriate adults to interact with minors.

The TAB was impressed not only with the goals of icouldbe.org but also with the end-to-end solution that they have implemented. Although the scale or their community is considerably smaller than the large social network sites and the goals of their online community are fundamentally different, we believe that icouldbe.org could serve as a model for the effective implementation of complementary technologies to enhance online safety for minors.

CONCLUSIONS

At the end of the review process, the TAB was overall encouraged by the innovation and energy apparent in this emergent technology area. Although no single technology provided a total solution to the various online safety problems facing minors as identified by the Research Advisory Board, each solution had some merit and some solutions could help a great deal. Further, it is clear that technology can play a role in keeping minors safer online by limiting sexual solicitation, online harassment, and access to problematic content, but it is also clear that technology alone is not enough given the nature of the challenges at hand. We are hopeful that the submitted technologies and any others in development will continue to evolve and improve in conjunction with progress on sociological fronts to optimize the mitigation of risks to minors on the Internet. We offer some concluding thoughts and recommendations below as a result of our review process.

Technology can play a role but cannot be the sole input to improved safety for minors online. Although Internet technology presents great benefits in terms of education, access to knowledge, and commerce, it of course allows social contacts and interactions that are not as easily monitored as on a supervised playground or other public space. Fortunately, with a combination of effective child and parent education, regular parental involvement or involvement by other responsible adults, continuing and increasing corporate responsibility, and some key software tools and technologies used in complement, we can as a society work to address online safety for minors more effectively.

The most effective technology solution is likely to be a combination of technologies. To the degree that online safety for minors can be addressed by technology on a standalone basis, the most comprehensive solution will likely require a several technologies working together in concert. Many of the submitted technologies were point solutions, addressing a part but not all aspects of safety for minors online. There was no single, all-encompassing solution, but this is not surprising, as online safety for minors is a multifaceted problem. Deploying complementary technology layers or using them in an end-to-end fashion will enhance the impact of any one single technology and will serve to maximize possible effectiveness.

Any and every technology solution has its limitations. No technology should be assumed to be foolproof upon deployment. In the realm of Internet safety, this is particularly true, as bad actors are likely to be especially motivated to circumvent technologies and as the stakes are extremely high. Further, some of the technologies can be circumvented as easily as a bad actor simply obtaining previously authorized credentials from an unsuspecting child.

Youth online safety measures must be balanced against concerns for the privacy and security of user information, especially information on minors. For virtually all submissions, regardless of the functional goal or type of technology, the storage and potential exposure of personal information were a potential concern. It is critical that appropriate privacy and security measures be implemented so that this amassed user

information is secure. Further, it is also important to understand the trade-off between potentially enhanced safety and the potential cost and precedent of providing private information – particularly on minors – to a possibly vulnerable or unreliable third party.

For maximum impact, client-side-focused technologies should be priced to enable all potential users to purchase and deploy them. Price points were frequently unclear or as yet unset from many of the submitted technologies. We would strongly urge innovative thinking in how to make client-side technologies as affordable as possible. Doing so will not only encourage and enable adoption by anyone concerned by children’s online safety and wishing to make technology part of their individualized solution, but will also generally encourage broad adoption, which can be critical to the effectiveness of some client-side technologies.

A common standard for sharing information among safety technologies would help. There is currently no open standard for sharing information voluntarily between users, sites, and third-party vendors interested in improving online safety for minors. It would be useful if an open data standard were defined for communication among the various classes of tools produced by different companies. This open standard should be developed with the participation of vendors, but without assuming specific server- or client-side technique and with a goal of protecting the privacy of users. To clarify, here is an example: using the standard, a server-based data-mining tool could flag conversations by sending data to the child’s computer; a parental-oversight tool might then be able to process this data to alert the parents. Development of this common standard would be an excellent next step in enhancing online safety for minors.

Developing standard metrics for youth online safety solutions would be useful. Standard metrics would assist in the assessment of the relative merits and trade-offs of any potential technology solution. Development of these metrics – no doubt a challenging process – would be an excellent next step in this process of seeking to enhance safety for minors online.

**Respectfully submitted to the Internet Safety Technical Task Force
on behalf of the Technology Advisory Board.**

Laura DeBonis, Chair, Technology Advisory Board

EXHIBITS TO APPENDIX D:

- 1. TAB Member and Observer Bios**
- 2. Submission Template**
- 3. Intellectual Property Policy**
- 4. Alphabetical List of Technology Submissions**

**Exhibit 1 to Appendix D:
TAB Member and Observer Bios**

EXHIBIT 1

TAB MEMBER BIOGRAPHIES

BEN ADIDA, HARVARD MEDICAL SCHOOL, HARVARD UNIVERSITY

Ben Adida is a member of the Faculty at Harvard Medical School and at the Children's Hospital Informatics Program, as well as a research fellow with the Center for Research on Computation and Society with the Harvard School of Engineering and Applied Sciences. His research is focused on security and privacy of health data, the security of web applications, and the design of secure voting systems.

Dr. Adida completed his PhD at MIT in the Cryptography and Information Security group. He is the Creative Commons representative to the W3C, working on interoperable web data as chair of the RDF-in-HTML task force. Previously, he co-founded two software startups that developed database-backed web application platforms based on free/open-source software.

SCOTT BRADNER, HARVARD UNIVERSITY

Scott Bradner has been involved in the design, operation and use of data networks at Harvard University since the early days of the ARPANET. He was involved in the design of the original Harvard data networks, the Longwood Medical Area network (LMAnet) and New England Academic and Research Network (NEARnet). He was founding chair of the technical committees of LMAnet, NEARnet and the COporation for Research and Enterprise Network (CoREN).

Mr. Bradner served in a number of roles in the IETF. He was the co-director of the Operational Requirements Area (1993-1997), IPng Area (1993-1996), Transport Area (1997-2003) and Sub-IP Area (2001-2003). He was a member of the IESG (1993-2003) and was an elected trustee of the Internet Society (1993-1999), where he currently serves as the Secretary to the Board of Trustees. Scott is also a trustee of the American Registry of Internet Numbers (ARIN).

Mr. Bradner is the University Technology Security Officer in the Harvard University Office of the Provost. He tries to help the University community deal with technology-related privacy and security issues. He also provides technical advice and guidance on issues relating to the Harvard data networks and new technologies to Harvard's CIO. He founded the Harvard Network Device Test Lab, is a frequent speaker at technical conferences, a weekly columnist for Network World, and does a bit of independent consulting on the side.

LAURA DEBONIS, BERKMAN CENTER, HARVARD UNIVERSITY

Laura DeBonis (Berkman Affiliate for the Internet Safety Technical Task Force). Laura chairs the Technology Advisory Board, which has been asked to assess the range of technology tools that may be used to promote online safety for minors. Laura was, most recently, the Director for Library Partnerships for Book Search at Google. During her time at the company, she also worked on the launch teams for AdSense Online and Froogle and managed global operations in the early days of Book Search. Prior to Google, Laura worked at Organic Online, consulting for a variety of companies on their web strategies and design. Before attending graduate school, she spent a number of years working in documentary film, video and interactive multimedia, creating content for PBS, cable channels, and museums. Laura is a graduate of Harvard College and has an MBA from Harvard Business School.

HANY FARID, DARTMOUTH

Hany Farid received his undergraduate degree in Computer Science and Applied Mathematics from the University of Rochester in 1989. He received his Ph.D. in Computer Science from the University of Pennsylvania in 1997. Following a two year post-doctoral position in Brain and Cognitive Sciences at MIT, he joined the Dartmouth faculty in 1999. Hany is the David T. McLaughlin Distinguished Professor of Computer Science and Associate Chair of Computer Science. He is also affiliated with the Institute for Security Technology Studies at Dartmouth. Hany is the recipient of an NSF CAREER award, a Sloan Fellowship and a Guggenheim Fellowship.

From working with federal law enforcement agencies on digital forensics, to the digital reconstruction of Ancient Egyptian tombs, Hany works and plays with digital media at the crossroads of computer science, engineering, mathematics, optics, and psychology.

LEE HOLLAAR, UNIVERSITY OF UTAH

Lee A. Hollaar is a Professor in the School of Computing (formerly the Department of Computer Science) at the University of Utah in Salt Lake City. He has taught a variety of software and hardware courses, and currently teaches computer networking, operating systems, and intellectual property and computer law.

He played a major role in adding two words to the vocabulary of intellectual property law:

- * "Inducement" was recognized by the Supreme Court in its unanimous Grokster opinion. The concept of liability for inducement of copyright infringement was revitalized in his paper Sony Revisited: A new look at contributory copyright infringement, and refined in his amicus brief in the case. The paper also led to the introduction of the Induce Act in the 108th Congress.

- * "Foreseeability" as a limit on doctrine of equivalents in patent law is the heart of the Supreme Court's Festo. It was proposed in the amicus brief whose filing he supervised as chair of IEEE-USA's intellectual property committee.

Professor Hollaar was on sabbatical leave in Washington, DC, during the 1996-97 academic year, as a Committee Fellow in the intellectual property unit of the Committee on the Judiciary of the United States Senate, where he worked on patent reform legislation, database protection, and what eventually became the Digital Millennium Copyright Act. He has been a special master, technical expert, or consultant in a number of copyright, patent, and trade secret cases.

Professor Hollaar was one of the drafters of the Utah Digital Signature Act, which made Utah the first government in the world to recognize digital signatures as equivalent to handwritten ones. On November 19, 1997, as part of Utah's Digital Signature Day, Professor Hollaar executed the first legally-recognized digitally-signed will in the world.

He received his BS degree in electrical engineering in 1969 from the Illinois Institute of Technology, and his PhD in computer science in 1975 from the University of Illinois at Urbana-Champaign. Dr. Hollaar was on the faculty of the University of Illinois prior to joining the faculty of the University of Utah in 1980.

TODD INSKEEP, BANK OF AMERICA

Todd Inskeep has over 20 years of Information Security and Internet experience ranging from secure radio and desktop systems to Security Architecture and eCommerce Authentication strategy at Bank of America. He's a Certified Information Systems Security Professional with a Master's in Strategic Intelligence currently leading work on the Bank's overall eCommerce/ATM strategy. He also teaches security & risk management part-time at the University of North Carolina at Charlotte's NSA-Designated Center of Excellence in Information Assurance. Todd

holds a BS in Electrical Engineering from West Virginia University and a MS in Strategic Intelligence from the Joint Military Intelligence College.

BRIAN LEVINE, UNIVERSITY OF MASSACHUSETTS-AMHERST

Brian Neil Levine is an Associate Professor in the Dept. of Computer Science at the Univ. of Massachusetts Amherst, which he joined in 1999. He received MS and PhD degrees in Computer Engineering from the Univ. of California, Santa Cruz in 1996 and 1999, respectively. His research focuses on networking and security, and he has published over 60 papers on these topics. In the networking area, his research focuses on mobile systems and peer-to-peer networking. In the security area, his research is focused on privacy and forensics. His lab is currently funded by the NSF, DARPA, NSA, and ARO. He received a National Science Foundation CAREER grant in 2002 for work in peer-to-peer networking, a prestigious award for new faculty. In 2004, he was awarded a UMass Lilly Teaching Fellowship and, in 2007, his college's Outstanding Teacher Award. In 2008, he received the Excellence in Science & Technology Alumni Award from the Univ. at Albany, where he received a B.S. in 1994. Levine is currently an associate editor of the IEEE/ACM Transactions on Networking journal.

ADI MCABIAN, TWISTBOX

Adi McAbian is Managing Director of Twistbox Entertainment and currently serves on the Board of Directors of Mandalay Media (MNDL), its parent.

Since founding the company, Mr. McAbian has been responsible for facilitating strategic collaborations with over 60 mobile operators worldwide on content standards and minor protection, he has been a frequent speaker, lecturing on adult mobile content business and management issues throughout Europe and the U.S. including conferences organized by iWireless World, Mobile Entertainment Forum, and Informa.

Mr. McAbian has worked with various operators including Vodafone's Global Content Standards group on establishing best practices in minor protection for both content and contact services as well as local implementations of those standards and supporting platforms in the over a dozen local markets. Mr. Mcabian also co-authored the Content Standards Rating Matrix currently used by nearly 100 networks to rate restricted content.

Mr. McAbian is responsible for corporate strategy and carrier relationships that span the globe.

Mr. McAbian's background includes experience as a successful entrepreneur and proven executive business leader with 12+ years as Business Development and Sales Manager in the broadcast television industry. Mr. McAbian is experienced in entertainment and media rights management, licensing negotiation and production, and has previously secured deals with AOL/Time Warner, Discovery Channel, BMG, RAI, Disney, BBC and Universal among others.

Mr. McAbian currently serves on the Mobile Marketing Associations' Consumer Best Practices Committee and will chair the up coming Age Appropriate Content and Services Sub-Committee.

RL "BOB" MORGAN, UNIVERSITY OF WASHINGTON

RL 'Bob' Morgan is Senior Technology Architect for the Computing & Communications Department at the University of Washington. In this role he contributes to designing, implementing, and documenting distributed computing and security infrastructure for the UW. He is the Chair of the Middleware Architecture Council for Education (MACE), providing guidance for the Internet2 Middleware Initiative. He is a primary contributor to a number of Internet2 middleware projects, notably Shibboleth, a system for secure access to inter-institutional web

resources. He is also active in standards activities with the Internet Engineering Task Force (IETF) and the Organization for the Advancement of Structured Information Standards (OASIS), where he has helped to develop the Lightweight Directory Access Protocol (LDAP) and Security Assertion Markup Language (SAML) standards.

LAM NGUYEN, STROZ FRIEDBERG

Lam Nguyen heads Stroz Friedberg's Digital Forensics lab in Boston. With over 11 years of coding, database development and digital forensics experience for leading government and commercial entities, Mr. Nguyen is an industry leader in digital forensics for data breach, e-discovery, and cybercrime in civil and criminal litigation, as well as corporate investigations. Mr. Nguyen has investigated hundreds of criminal cases and has led forensic investigations in data breach and intrusion cases. He was the lead investigator in several searches for Personally Identifiable Information on lost and stolen computers for a large pharmaceutical company. Mr. Nguyen recently conducted a forensic examination of an employee's computer for a large investment bank. That examination led to his testimony in federal court that helped prove the employee was engaged in insider trading.

Before joining Stroz Friedberg, Mr. Nguyen was the Lead Computer Forensics Specialist for the United States Department of Justice, Child Exploitation and Obscenity Section's High Technology Investigative Unit. As the team leader, he initiated and developed online investigations of high-profile child exploitation cases; examined target computers seized in criminal investigations, and provided his expertise to federal prosecutors across the country. Mr. Nguyen is highly respected in the digital forensic community and has been qualified as an expert in federal court on a number of occasions.

Sought after for his exceptional experience and commitment, he has trained law enforcement officers and trial attorneys on computer forensic issues domestically and abroad. Mr. Nguyen was an adjunct instructor at George Mason University for several years where he developed new courses and curricula on the subject of Computer Forensics and Network Security. More recently, he has been a guest lecturer at Harvard Law, Harvard Extension School, and the University of Massachusetts at Amherst.

Mr. Nguyen's dedication to public service has also included coordinating and delivering technology solutions critical to the operations of the U.S. Dept. of Commerce, Bureau of the Census, U.S. Dept. of Treasury, and Internal Revenue Service. Mr. Nguyen earned his Masters of Information Technology from American Intercontinental University and his undergraduate degree in Accounting Information Systems from Virginia Tech. He is certified in EnCase.

JEFFREY SCHILLER, MIT

JEFFREY I. SCHILLER received his S.B. in Electrical Engineering (1979) from the Massachusetts Institute of Technology. As MIT Network Manager he has managed the MIT Campus Computer Network since its inception in 1984. Prior to his work in the Network Group he maintained MIT's Multics timesharing system during the time-frame of the ArpaNet TCP/IP conversion. He is an author of MIT's Kerberos Authentication system. From 1994 through 2003 Mr. Schiller was the Internet Engineering Steering Group's (IESG) Area Director for Security, responsible for overseeing security related Working Groups of the Internet Engineering Task Force (IETF). He was responsible for releasing a U.S. legal freeware version of the popular PGP encryption program.

Mr. Schiller is also responsible for the development and deployment of an X.509 based Public Key Infrastructure (PKI) at MIT. He serves as a consultant to other higher educational institution in the usage and deployment of PKI and related security technologies.

Mr. Schiller is also a founding member of the Steering Group of the New England Academic and Research Network (NEARnet). NEARnet, now part of Level3, is a major nationwide Internet Service Provider.

DANNY WEITZNER, MIT

Daniel Weitzner is Policy Director of the World Wide Web Consortium's Technology and Society activities. As such, he is responsible for development of technology standards that enable the web to address social, legal, and public policy concerns such as privacy, free speech, security, protection of minors, authentication, intellectual property and identification. Weitzner holds an appointment as Principal Research Scientist at MIT's Computer Science and Artificial Intelligence Laboratory, co-directs MIT's Decentralized Information Group with Tim Berners-Lee, and teaches Internet public policy at MIT.

As one of the leading figures in the Internet public policy community, he was the first to advocate user control technologies such as content filtering and rating to protect children and avoid government censorship of the Internet. These arguments played a critical role in the 1997 US Supreme Court case, *Reno v. ACLU*, awarding the highest free speech protections to the Internet. He successfully advocated for adoption of amendments to the Electronic Communications Privacy Act creating new privacy protections for online transactional information such as Web site access logs.

Before joining the W3C, Mr. Weitzner was co-founder and Deputy Director of the Center for Democracy and Technology, a leading Internet civil liberties organization in Washington, DC. He was also Deputy Policy Director of the Electronic Frontier Foundation. He serves on the Boards of Directors of the Center for Democracy and Technology, the Software Freedom Law Center, the Web Science Research Initiative, and the Internet Education Foundation.

His publications on technical and public policy aspects of the Internet have appeared in the *Yale Law Review*, *Science* magazine, *Communications of the ACM*, *Computerworld*, *Wired Magazine*, and *The Whole Earth Review*. He is also a commentator for NPR's *Marketplace Radio*.

Mr. Weitzner has a degree in law from Buffalo Law School, and a B.A. in Philosophy from Swarthmore College.

TAB OBSERVER BIOGRAPHIES

RACHNA DHAMIJA, USABLE SECURITY SYSTEMS

Dhamija's research interests span the fields of computer security, human computer interaction and information policy. She received a Ph.D. from the School of Information Management and Systems at U.C. Berkeley in 2005. Her thesis focused on the design and evaluation of usable security systems. Previously, Dhamija worked on electronic payment system privacy and security at CyberCash. Her research has been featured in the *New York Times*, the *Wall Street Journal* and the *Economist*.

EVIE KINTZER, WGBH

Evie Kintzer, is WGBH Educational Foundation's Director of Strategic Planning and Special Projects. For the last eight years, Evie's work with the President and Vice Presidents has included developing the Foundation's strategic planning agenda, assessing implications of the

competitive environment, chairing WGBH's Advanced Media Group, and advising and developing project strategy and operating plans. Evie spent 13 years in the WGBH Legal Department as Director of Business Affairs and Deputy General Counsel, handling all of the business and legal affairs issues related to documentary programs produced by American Experience, NOVA, and FRONTLINE, as well as development of the Children's Television and Interactive Departments. She holds a BA from Brandeis University and a JD from Hastings College of the Law.

AL MARCELLA, WEBSTER UNIVERSITY

Albert J. Marcella Jr., is president of Business Automation Consultants, LLC a global information technology and management-consulting firm providing information technology (IT) management consulting and IT audit and security reviews and training for an international clientele.

Dr. Marcella is an internationally recognized public speaker, researcher, workshop and seminar leader with 30 years of experience in IT audit, security and assessing internal controls, and an author of numerous articles and 28 books on various IT, audit and security related subjects.

Dr. Marcella's most recent book *Cyber Forensics: Collecting, Examining, and Preserving Electronic Evidence An Auditor's Field Manual*, second edition, focuses on issues, tools, and control techniques designed to assist audit, law enforcement, and info security professionals in the successful investigation of illegal activities perpetrated through the use of information technology.

Professor Marcella is a tenured faculty member at Webster University in Saint Louis, MO, where he is responsible for teaching information technology management courses in the University's graduate and doctoral programs.

Dr. Marcella is the Institute of Internal Auditors Leon R. Radde Educator of the Year, 2000, Award recipient. Dr. Marcella has taught IT audit seminar courses for the Institute of Internal Auditors, continues to teach for the Information Systems Audit and Control Association, and has been recognized by the IIA as a Distinguished Adjunct Faculty Member.

JOHN MORRIS, CDT

John B. Morris, Jr. is CDT's General Counsel, and the Director of its "Internet Standards, Technology and Policy Project." Prior to joining CDT in 2001, Mr. Morris was a partner in the law firm of Jenner & Block, where he litigated groundbreaking cases in Internet and First Amendment law. He was a lead counsel in the ACLU v. Reno/American Library Association v. U.S. Dep't of Justice case, in which the Supreme Court unanimously overturned the Communications Decency Act of 1996 and extended to speech on the Internet the highest level of constitutional protection. In that case, Mr. Morris was responsible for the development of the factual presentation concerning how the Internet works, a presentation that served as the foundation for the Supreme Court's landmark decision.

From May 1999 through April 2000, Mr. Morris served as director of CDT's Broadband Access Project (while on leave from his firm). The Project undertook a comprehensive assessment of the legal, policy, and factual issues surrounding the emergence of broadband Internet access technologies.

Prior to becoming a lawyer, Mr. Morris had extensive experience with computers and politics. In the mid-1970's, as a staff member on Capitol Hill, he helped to promote the use of computer software to manage and improve constituent communications. In 1981, Mr. Morris joined a D.C.-area computer company, where he was one of the lead system designers of a constituent management software system for Members of Congress. In 1985, he co-founded Intelligent

Solutions, Inc., which developed the leading constituent services product used on Capitol Hill today.

Mr. Morris received his B.A. magna cum laude with distinction from Yale University and his J.D. from Yale Law School, where he was the Managing Editor of the Yale Law Journal. Following law school, he clerked for Judge Thomas A. Clark of the Eleventh Circuit Court of Appeals, worked for three years as a staff attorney at the Southern Center for Human Rights in Atlanta, Georgia, and then joined Jenner & Block in Washington in 1990.

In addition to his work with CDT, Mr. Morris is an Adjunct Professor of Law at Cardozo Law School in New York City.

TERESA PILIOURAS, POLYTECHNIC UNIVERSITY

Teresa Piliouras is an Adjunct Professor in Computer and Information Science/Technology Management at Polytechnic University, where she has taught courses in network design, bioinformatics, network security, operations research, operations management, database design, and management of technology since 1994. The department participates in four interdisciplinary research centers and houses a number of departmental labs and research groups (<http://www.poly.edu/cis/research/labs/index.php>) which are funded by grants from government agencies such as the National Science Foundation, NASA, the Office of Naval Research, the Air Force, and the New York State Office of Science, Technology, and Academic Research, and private companies and foundations such as IBM, Hewlett-Packard, AT&T, the Sloan Foundation, Panasonic, Intel, and Verizon. The Information Systems and Internet Security (ISIS) Laboratory consists of heterogeneous platforms and multiple interconnected networks to facilitate experimentation in issues related to information security. ISIS was designated an NSA Center of Excellence in 2002. It is currently further being expanded with an NSF Scholarship for Service (SFS) capacity building grant and is the host laboratory for Polytechnic University's SFS program.

Dr. Piliouras is working on ways to protect children on the Internet and to promote public health. She is involved in a number of broad-based community outreach programs to bring seniors and "at-risk" youth together to address problems of health and wellness. This involves creating community wiki-webs designed to create a sense of support and community, especially among those who may have been marginalized in the past. She is founder and President of Albright Associates, a company dedicated to protecting the privacy and safety of children in digital environments. Prior to Albright Associates, she was founder of TCR, Inc., a consulting company specializing in data mining and advanced intelligent technologies. She also held executive and technical positions at Accenture, Pitney Bowes, Boehringer Ingelheim, and Pepsico. She holds a Bachelor of Science from the University of Illinois, a Masters of Business Administration from Iona College, a Ph.D. from Polytechnic University, and a Postdoctoral Fellow from the Man-Machine Institute. She has authored numerous scholarly books and articles, including "Network Design: Management and Technical Perspectives" and "CRC Press Handbook of Modern Telecommunications."

GREG RATTRAY, COL (RET), DELTA RISK

Currently, Greg Rattray is a Principal, Delta Risk Consulting, establishing risk management strategies and cyber security capacity building approaches for government and private sector clients and advising the Internet Corporation for Assigned Names and Numbers (ICANN) on approaches for enhancing global Internet security. Previously, Greg served 23 years as an U.S. Air Force officer, retiring in summer 2007. His assignments included Director for Cyber Security on the White House National Security Council staff, leading national policy development & NSC oversight for cyber security programs and oversight of Iraq telecommunication reconstruction. He commanded the Operations Group of the AF Information Warfare Center responsible for global

operations of 900 personnel/\$100 million active duty and National Guard team responsible for Air Force-wide tactics, red teams, exercising, test & training. He served in a number of operational intelligence and information operations assignments from the unit to Headquarters, Air Force levels. He also served as an Assistant Professor of Political Science and Deputy Director of the USAF Institute of National Security Studies at the Air Force Academy. He is the author of numerous books and articles including Strategic Warfare in Cyberspace, a seminal work in the cyber conflict field. He received his Ph.D. from Fletcher School of Law & Diplomacy, Tufts University, his Masters in Public Policy from J. F. Kennedy School of Government, Harvard University and his B.S. from U.S. Air Force Academy. He is a full member of the Council on Foreign Relations.

JEFF SCHMIDT, CONSULTANT

Jeff Schmidt is an independent security and technology risk consultant focusing on identity-related issues. Previously, Jeff founded Secure Interiors (SI), an early provider of managed Internet security services, and Authis, a provider of innovative identity services for the financial vertical. He managed both business to successful acquisition. Jeff also assisted in the re-launch of Kleiner Perkins backed ENDFORCE (formerly SmartPipes) by managing their flagship product offering to initial revenue generation. ENDFORCE was subsequently acquired by Sophos. Jeff also served as the CIO of The Ohio State University's second largest business unit and spent time at The Microsoft Corporation where he spearheaded Microsoft's first internal malicious testing of Windows 2000.

Jeff is a founder and elected Director of the InfraGard National Members Alliance, the private sector component of the FBI's InfraGard Program (InfraGard is an FBI/private sector alliance dedicated to improving and extending information sharing between private industry and the government on matters of national security). Jeff helped the FBI create the InfraGard Program in 1998 and has received commendations from the Attorney General, the Director of the FBI, and the National Infrastructure Protection Center (NIPC - now a part of the Department of Homeland Security).

On topics of computer security, Jeff is frequently interviewed and cited by numerous national publications and news outlets. He has authored several scholarly papers and has testified before state legislative bodies and the United States Congress. Jeff is a frequent speaker at major events such as Microsoft's DevDays, ITEC, ISSA, InfraGard, and Conference Board events.

Jeff authored The Microsoft Windows 2000 Security Handbook, published by Que in four languages, and contributed to Using Windows NT 4.0, and Teach Yourself Linux in 10 Minutes, also published by Que. He received a BS CIS from The Ohio State University and an MBA Magna Cum Laude from the Fisher College of Business at The Ohio State University.

JOHN SHEHAN, NCMEC

John Shehan is the Director of Exploited Children Services (ECS) at the National Center for Missing & Exploited Children (NCMEC) in Alexandria, Virginia. He is responsible for policy decisions and the overall operations within the ECS. Mr. Shehan has been with NCMEC since February, 2000 and has participated in and presented at numerous law enforcement investigative training programs on high technology crimes, online child exploitation as well as investigative and analytical skill development. He has provided extensive technical assistance to law enforcement in the United States and abroad on cases of child sexual exploitation, especially Internet crimes against children. To raise awareness of online child sexual exploitation, he speaks regularly with media outlets such as the MSNBC, CBS World News, New York Times, CNN and others.

Mr. Shehan is an active and founding member of the Financial Coalition Against Child

Pornography. He, along with other members at NCMEC collaborated to develop CyberTipline III. This system enables participating financial institutions and law enforcement to share information with an ultimate goal of eradicating the commercial viability of child pornography. John also spearheaded and manages the NetSmartz411 program. This program educates adults on all aspects of computers, the Internet and Internet safety.

NCMEC's Exploited Children Services was established in 1996 by a mandate by the United States Congress. ECS works collaboratively with the Federal Bureau of Investigation, U.S. Postal Service, U.S. Department of Justice, and the U.S. Customs Service (now the Department of Homeland Security) in cases of child sexual exploitation. ECS serves as a resource center for the public, parents, law enforcement, and others on the issues of the sexual exploitation of children. ECS analysts process reports received on the sexual exploitation of children through the CyberTipline and disseminate the leads to federal, state, local and international law enforcement agencies for further investigation. ECS analysts provide technical assistance to federal, state, local, and international law enforcement agencies investigating child sexual exploitation cases.

**Exhibit 2 to Appendix D:
Submission Template**

Internet Safety Technical Task Force Technology Submission Template

Company Name / Individual
<http://www.website.com>

PLEASE SUBMIT BY JULY 21, 2008

ABSTRACT

This template describes the formatting and content requirements for submissions to the Internet Safety Technical Task Force's Technical Advisory Board. (This format should be familiar to any technologist who has submitted to ACM publications.) Please follow the structure of the template below. If necessary, please repeat information to accord with the template questions and layout. *Please note: Your submission should be no longer than four pages including diagrams and bibliography.*

Keywords

Provide 1-5 keywords to describe the submitted technology. Sample keywords that might be useful in this context are: filtering, searching, identification, verification, parental controls, and forensics.

Functional Goals

Please indicate the functional goals of the submitted technology by checking the relevant box(es):

- Limit harmful contact between adults and minors
- Limit harmful contact between minors
- Limit/prevent minors from accessing inappropriate content on the Internet
- Limit/prevent minors from creating inappropriate content on the Internet
- Limit the availability of illegal content on the Internet
- Prevent minors from accessing particular sites without parental consent
- Prevent harassment, unwanted solicitation, and bullying of minors on the Internet
- Other – please specify

PROBLEM INTRODUCTION

Briefly introduce the problem being addressed, citing any relevant studies. Briefly introduce the proposed solution. If the submitted technology addresses multiple problems (e.g. has multiple goals per the subsection above), please list separately each problem-solution combination.

PROPOSED SOLUTION

Describe the technical solution being proposed. Again if the technology addresses multiple problems with each a separate solution, please address each solution separately. This solution description should include enough detail to allow an assessment of whether or not the proposed solution could solve the problem being addressed. The audience for this description will be computer scientists,

security experts, and engineers. When in question, the authors should err on the side of being more technical rather than less. The submission should resemble an ACM/IEEE submission in both style and substance.

In Addition to the Above Description, Please Address Each of the Following:

- Describe the solution's technical attributes, e.g. features and functionality.
- Provide use cases.
- Specify what the technology successfully solves and what it does not. Describe how the technology's effectiveness is evaluated, measured, and tested.
- Provide a strengths-weaknesses analysis.
- Detail the implementation requirements (hardware, software, end user aptitudes).
- Describe the technical standards used in implementing the proposed technology and identify the standards bodies that are the home of existing or proposed future standards.
- Discuss the technology's reliance and use of law and policy for success.
- Discuss the viability of the technology in both the US and international context.
- Detail effectiveness to date. Please provide any information possible on "failures" of the technology.

EXPERTISE

Describe the expertise of the company/developers. If appropriate, indicate other clients and products in this space.

COMPANY OVERVIEW

Please provide a description of the company including but not limited to information about founders and key team members, sources of capital, revenue (if relevant), customer base, growth, partnerships, participation in standards bodies, etc. Information submitted in this section will vary depending on a company/organization's stage in lifecycle. Our goal is to understand the context around the technology you have submitted for review.

BUSINESS MODEL OVERVIEW

Please discuss direct and indirect costs to all potential users. Please also comment on distribution model to non-profits, start-up sites and services, and other organizations that might not be able to afford full price for this technology. Our goal is to understand financial

accessibility and cost implications for all existing and new players.

MORE INFORMATION

Feel free to provide a URL that readers can go to for more information. This may include videos, detailed specs, or anything else that might be relevant. Indicate in this document what the readers might find if they go to the URL. This is a great place for information you would like to include that does not otherwise fit the structure of this document.

CONTACT INFORMATION

The final section of this document should contain basic contact information, including a contact name, email, phone number, and address for follow up. Please send any relevant additional information about contacting the people listed here to tab@cyber.law.harvard.edu.

CERTIFICATION

At the end of your submission, you should include the following statement: "I certify that I have read and agree to the terms of the Internet Safety Technical Task Force Intellectual Property Policy." The IP Policy can be found at <http://cyber.law.harvard.edu/research/isttf/ippolicy>.

USE OF THIS DOCUMENT

This document should not contain information that cannot be made available to the public. (See Legal Notice below) This submission will be made available to the Technical Advisory Board, the Task Force, and the Attorneys General. Additionally, after initial review, submissions may be made public and published online for public commentary. Please note that you must be prepared, in any follow-up discussions on your submission with the Task Force, to provide sufficient, non-confidential details and explanation about how your technical solution works and upon what information it relies, in order to allow the Task Force meaningfully to evaluate your solution.

NOTE: THE SUBMISSION TEMPLATE ENDS HERE -- FORMAT INSTRUCTIONS FOLLOW BELOW. PLEASE DELETE THE FORMAT INSTRUCTIONS FROM YOUR DOCUMENT PRIOR TO SUBMISSION. THEY DO NOT COUNT AS PART OF THE FOUR PAGE SUBMISSION LIMIT.

INSTRUCTIONS

FORMAT INFORMATION

This template is modified from the template used by the Association for Computing Machinery (ACM) and, specifically, the Special Interest Group in Computer-Human Interaction (SIGCHI). By conforming to this template, we are able to provide reviewers and the public with a collection of documents that allow for easy reviewing.

All material on each page should fit within a rectangle of 18 x 23.5 cm (7" x 9.25"), centered on the page, beginning 1.9 cm (.75") from the top of the page, with a .85 cm (.33"). *Your submission should be no longer than four pages including diagrams and bibliography.*

Normal or Body Text

Please use 10-point Times Roman font, or other Roman font with serifs, as close as possible in appearance to Times Roman in which these guidelines have been set. The goal is to have a 10-point text, as you see here. Please use sans-serif or non-proportional fonts only for special purposes, such as distinguishing source code text. The Press 10-point font available to users of Script is a good substitute for Times Roman. If Times Roman is not available, try the font named Computer Modern Roman. On a Macintosh, use the font named Times.

Title and Authors

The title (Helvetica 18-point bold), authors' names (Times Roman 12-point bold) and affiliations (Times Roman 12-point) run across the full width of the page – one column 17.8 cm (7") wide.

Abstract and Keywords

Every submission should begin with an abstract of about 100 words, followed by a set of keywords. The abstract and keywords should be placed in the left column of the first page under the left half of the title. The abstract should be a concise statement of the problem and approach of the work described.

Subsequent Pages

For pages other than the first page, start at the top of the page, and continue in double-column format. Right margins should be justified, not ragged. The two columns on the last page should be of equal length.

References and Citations

Use the standard Communications of the ACM format for references – that is, a numbered list at the end of the article, ordered alphabetically by first author, and referenced by numbers in brackets [1]. See the examples of citations at the end of this document. Within this template file, use the style named references for the text of your citation. References should be published materials accessible to the public. Internal technical reports may be cited only if they are easily accessible (i.e. you can give the address to obtain the report within your citation) and may be obtained by any reader. Proprietary information may not be cited. Private communications should be acknowledged, not referenced (e.g., "[Robertson, personal communication]").

Page Numbering, Headers and Footers

Do not include headers, footers or page numbers in your submission.

SECTIONS

The heading of a section should be in Helvetica 9-point bold in all-capitals. Sections should be unnumbered.

Subsections

The heading of subsections should be in Helvetica 9-point bold with only the initial letters capitalized. (Note: For subsections and subsubsections, a word like the or a is not capitalized unless it is the first word of the header.

Subsubsections

The heading for subsubsections should be in Helvetica 9-point italic with initial letters capitalized.

FIGURES

Figures should be inserted at the appropriate point in your text. Figures may extend over the two columns up to 17.8 cm (7") if necessary. Each figure should have a figure caption in Times Roman.

LANGUAGE, STYLE AND CONTENT

Please write for a well-informed, technical audience, but try to make your submission as clear as possible:

- Briefly define or explain all technical terms.
- Explain all acronyms the first time they are used in your text.

- Explain “insider” comments. Ensure that your whole audience understands any reference whose meaning you
- do not describe (e.g., do not assume that everyone has used a Macintosh or a particular application).
- Use unambiguous forms for culturally localized concepts, such as times, dates, currencies and numbers (e.g., “1-5- 97” or “5/1/97” may mean 5 January or 1 May , and “seven o'clock” may mean 7:00 am or 19:00).

REFERENCES

1. Anderson, R.E. Social impacts of computing: Codes of professional ethics. *Social Science Computing Review* 10, 2 (Winter 1992), 453-469.
2. CHI Conference Publications Format. Available at <http://www.acm.org/sigchi/chipubform/>.
3. Conger., S., and Loch, K.D. (eds.). Ethics and computer use. *Commun. ACM* 38, 12 (entire issue).
4. Mackay, W.E. Ethics, lies and videotape, in *Proceedings of CHI '95* (Denver CO, May 1995), ACM Press, 138-145.
5. Schwartz, M., and Task Force on Bias-Free Language. *Guidelines for Bias-Free Writing*. Indiana University Press, Bloomington IN, 1995.

The columns on the last page should be of equal length.

PLEASE SUBMIT YOUR FINAL DOCUMENT AS A PDF

LEGAL NOTICE

The Berkman Center, the Task Force and Task Force members, and the Technical Advisory Board, including its members and affiliates, are under no obligation to maintain the confidentiality of the submitted abstracts or other materials you provide. Please do not submit any information in your technical abstract that is confidential, proprietary or not for public dissemination. Please submit only information that you are willing to have made public. All submissions are subject to the Task Force Intellectual Property Policy: <http://cyber.law.harvard.edu/research/isttf/ippolicy>. By submitting your abstract or proposal, you certify that you have read and agree to the terms of that Policy.

**Exhibit 3 to Appendix D:
Intellectual Property Policy**

Intellectual Property Policy for the Internet Safety Technical Task Force

This IP policy is intended to state the manner in which intellectual property presented or submitted to the Task Force will be handled and to clarify that no confidentiality obligations will be imposed on Task Force members.

No Confidentiality of Contributions

No contribution or presentation by any Task Force member or non-member contributor to the Task Force regarding any research, technology or service (hereinafter “Submission”) will be treated as confidential. Task Force members and the Technical Advisory Board, including its members and observers, shall have no duty to maintain the confidentiality of, and shall not execute or be subject to any confidentiality agreement for, such Submissions. Contributors should not present, and the Task Force will not accept, any information in a Submission that is confidential, proprietary or otherwise not for public dissemination. Contributors should submit only information that they are willing to have made public. Contributors must be prepared, in any follow-up discussions with the Task Force or the Technical Advisory Board to their initial Submission, to provide sufficient, non-confidential details and explanation about how their proposed technology or service works and upon what information it relies to allow the Task Force meaningfully to evaluate their Submission; otherwise the Task Force may not be able to continue to assess that Submission and include it in any reports.

Copyrighted Materials

Task Force members and non-member contributors will retain copyright in their Submissions to the Task Force. By providing your Submission to the Task Force, you are granting the Berkman Center and the Task Force a non-exclusive, royalty-free, perpetual, irrevocable and worldwide license to use your Submission for the sole purposes of carrying out the Task Force’s work and developing the Task Force’s reports, including, without limitation, the license rights to store, copy, distribute, transmit, publicly display, publicly perform, reproduce, edit, translate and reformat your Submission, and/or to incorporate it into a collective work. The Berkman Center and the Task Force shall have no obligation to publish, disseminate, incorporate in Task Force reports, or make any other use of any Submission.

Task Force members and non-member contributors understand that they may currently or in the future be developing internally information eligible for copyright, or receiving such information from other parties, that may be similar to the materials furnished in Submissions. Participation in this Task Force shall not in any way limit, restrict or preclude any Task Force member from pursuing any of its present or future copyright activities or interests or from entering into any copyright agreement or business transaction with any person.

Patents

Task Force members and non-member contributors will retain all pre-existing patent rights in their Submissions to the Task Force. No license, express or implied, of any patent owned by the contributors disclosed during this Submissions process is granted. Task Force members and non-member contributors understand that they may currently or in the future be developing patentable information internally, or receiving patentable information from other parties, that may be similar to the patents disclosed during this process. Participation in this Task Force shall not in any way limit, restrict or preclude any Task Force member from pursuing any of its present or future patent activities or interests or from entering into any patent agreement or business transaction with any person.

Trade Secrets

Because Task Force members and the Technical Advisory Board, including its members and observers, will be under no obligation to maintain the confidentiality of Submissions, any material that a contributor considers to be a trade secret or otherwise confidential or proprietary should not be submitted to the Task Force or the Technical Advisory Board.

Intellectual Property Created by the Task Force

All intellectual property in any Task Force report, except that in Submissions by Task Force members contained in such reports, shall be owned by the Berkman Center. The Berkman Center will grant to each Task Force member an appropriate, non-exclusive, royalty-free, perpetual, irrevocable and worldwide license to store, copy, distribute, transmit, publicly display, publicly perform, reproduce, edit, translate, and/or reformat the contents of any Task Force report for the purposes of facilitating or carrying out that member's participation in the Task Force and activities related to the work of the Task Force.

**Exhibit 4 to Appendix D:
Alphabetical List of Technology Submissions**

EXHIBIT 4

SUBMISSION LIST

1. ALIAS
2. Appen Speech Language Technology: Data Stream Profiling
3. Appen Speech Language Technology: Text Attribution Tool
4. Aristotle
5. AssertID
6. Been Verified
7. Chatsafe - Carmichael Group
8. Chatsafe-Crystal Reference Systems
9. CheckMyAge
10. Choicepoint
11. Covenant Eyes: Accountability
12. CovenantEyes: Accountability and Filter
13. CredInt
14. DeepNine
15. eGuardian
16. EthoSafe
17. Gemalto
18. GenMobi Technologies
19. Icouldbe.org
20. IDology
21. Infoglide
22. InternetSafety.com
23. Keibi
24. Kidsnet
25. McGruffSafeGuard
26. Microsoft
27. Net Nanny / Content Watch
28. NetIDme
29. Portcard
30. Privo-Parity: Privacy Vaults Online
31. Privo-Parity:KidCards
32. PureSight
33. RedStarhs
34. RelyID
35. Saferspace
36. Sentinel: ADAPT
37. Sentinel: SAFE
38. Spectorsoft
39. Symantec
40. Verifcage

APPENDIX E:

Submissions from Social Network Sites

Internet Technical Safety Taskforce – Request for Input Bebo and AOL

Bebo and AOL are pleased about the opportunity to provide the Internet Technical Safety Task Force with input ahead of its final report. This response provides an overview of Bebo's approach to safety on its social network, as well as the more general approach taken by AOL in its other Internet services.

What safety issues do you attempt to address on your site?

Excluding the more universal online threats including virus, spyware, spam and phishing, there are two sets of child protection issues that Bebo and AOL work to address in our respective services. When assessing risk, we consider:

1. Traditional categories of potential online risk, which include conduct, content, and contact; and
2. Young people becoming perpetrators as well as the victims of harm.

Categories of Potential Online Risk: These categories include:

1. Inappropriate content, which includes exposure through the Internet to pornography, violence, racist content, misinformation and propaganda that can negatively impact young people.
2. Inappropriate contact, which includes contact between adults with a sexual interest in children, or by young people who solicit other young people.
3. Inappropriate conduct, which relates to how young people behave online through social networks. Problems here include:
 - a. Bullying or victimization, which includes behaviors such as spreading rumors, excluding peers from one's social group, and withdrawing friendship or acceptance, or
 - b. Risk-seeking behaviors, which includes, divulging personal information, posting sexually provocative photographs, lying about real age or arranging to meet face-to-face with people only ever previously met online.

Young People as Perpetrators: One of the central features of Web 2.0 is the increasingly active role of young people as producers, publishers and disseminators of content. Although much of this activity produces beneficial content, it is also important to remember that young people can initiate or participate in harmful activities, such as cyberbullying and cyberstalking. This fact needs to be taken into consideration when proposing safeguards and solutions.

How do you measure the risk that youth face on your site?

AOL and Bebo assess risk first at the product development stage and then on an ongoing basis, and then develop and assess the available solutions. We calculate risk based on assessment of certain factors that may be present in a particular service, such as the following:

1. Is there interactivity through service such as chat, IM, and email?
2. Does the service offer file sharing or storage capability?
3. Is there a search component?
4. What content can users post through services such as text, graphics, audio, videos?
5. Is it a public or private service?
6. Who is the target audience? Is the service intended for a teen or adult audience?
7. What is the level of interaction between adults and minors?
8. What information is collected, either actively or passively?
9. What are the access points to the service?

By analyzing these factors and identifying the pertinent risks, it is then possible to apply technology and industry safety recommendations to mitigate the risks. The risk assessment process provides an opportunity to develop innovative and bespoke safety features.

Risk evaluation is an ongoing process. Bebo and AOL have online safety teams involved in product development. These teams integrate a combination of user protections, empowerment tools, reporting capability, safety messaging, and enforcement to reduce risk to our customers. The teams also monitor activity on a particular service after it is launched in order to adjust policies and enforcement as necessary.

What technical (and non-technical) efforts have you undertaken to make your site safer for youth? Please list all features, policies, collaborations, etc. Indicate which safety issues these efforts attempt to address and which age groups are targeted in this approach. Please note if these are in-house efforts or if they are outsourced or a part of a collaboration and, if so, who your partners are. For each effort, please indicate your metrics for success.

Both Bebo and AOL are leaders in online child protection and have developed a strong set of Internet safety tools for use on our services by our customers, as well as a strong collaboration with law enforcement.

BEBO

For its social network, Bebo has developed a holistic three-pronged approach to risk management by attempting to *secure the service*, *support users* and implementing proactive and reactive *crime prevention strategies*.

1. *Helping Secure the Bebo Service*

Terms of Use and Other Policies: Bebo has Terms of Service that clearly outline unacceptable user conduct and content. Our Privacy Policy outlines what data is collected, how it is used and how users can change their privacy settings. Both policies can be reached from any page on the site.

Safety Features: Bebo has been an active participant on the UK Home Office Internet Task Force that developed the Good Practice Guidelines for Social Networking and User Interactive Services. Bebo adheres to the guidelines laid out in this document. It is worth noting that many safety features on Bebo pre-date the guidance. The following are some examples of Bebo's safety features:

- a. All profiles on Bebo are Private by default meaning only "friends" may view the profile.
- b. It is not possible to search for users under the age of 16 using search engines.
- c. Users are given the ability to block other users.
- d. Users are able to review comments before they appear on their profile.
- e. Users are restricted from re-registering with a false age if they have previously attempted to register with an underage date of birth.
- f. Users are able to view and alter their privacy settings at any time; they can change their profile from public to private (and vice versa); they can allow only friends to post comments on their profile; they can hide the number of times their profile has been viewed; they can restrict the age range of people able to contact them.
- g. Users can delete their accounts and thereby their profiles.

Proactive Efforts: In addition to responding to user reports of inappropriate content, Bebo proactively seeks out inappropriate content using software and other mechanisms to review such content (which includes video content and thumbnail images).

2. *Supporting User Education and Well-Being*

Education: To help users to enjoy the Bebo site in a safe and responsible way, Bebo provides education and tips about online safety and privacy in clear and relevant language throughout the site:

Bebo places a link to its safety page on every page on the site, bebo.com/safety as well as featuring links to relevant online safety and security resources. The safety page features a series of animations on topics. These animations, which are continually reviewed and updated, were created in consultation with young people and parents to ensure that they were accessible and clear.

Bebo also places context specific safety messages in areas where young people make decisions about how to interact with the community. For example, when users register they are strongly advised to keep their profile Private if they are under 21. When users sign in to use the service their IP address is visible with messaging which details that they are not anonymous online.

Bebo has also worked with teachers and education authorities to develop materials and lesson plans specifically for teachers. These are available from the dedicated website safesocialnetworking.com. Bebo took part in an industry led education initiative <http://en.teachtoday.eu>, which sought to address the potential knowledge gap between teachers and their students regarding new technologies. Although the site was developed as part of a European project, the guidance that is offered is equally applicable to teachers and education professionals around the world.

Well-Being: In addition to providing safety and privacy education to our users, we believe that social networks such as Bebo have huge potential to positively help young people address broader issues in their lives. Research findings indicate that many teenagers fall prey to abuse both offline and online without ever having violated applicable laws. For others, personal attributes render them vulnerable both to law breaking and victimization. Bebo has therefore created a site called [Be Well](http://www.bebo.com/bewell) (www.bebo.com/bewell). This is a well-being center, which allows support providers to use the Bebo platform as a means to access young people in need of their services. Bebo has partnerships with support organizations on issues such as depression, self-harm, drugs and eating disorders. Our goal is to help provide support to those who have fallen victim to abuse and to empower young people with the knowledge to identify possible risks to their personal safety and well-being and to seek appropriate help to mitigate those risks.

In addition, Bebo is heavily involved in the Technology for Well-Being good practice policy group. This group brings together a number of stakeholders, including, representatives from the technology, research and non-profit sectors to explore opportunities to work collaboratively in developing initiatives that harness the power of the Internet and related technologies to improve wellbeing. Web 2.0 offers mental health, social care and support service providers a myriad of positive opportunities to educate and raise awareness of the services offered to young people, as well as deliver those services from within an online community.

3. Crime Prevention Strategies

Bebo operates a robust Report Abuse system, and actively encourages users to report any breach of Terms or any other behavior or content that they find inappropriate. Every profile page contains a Report Abuse link located underneath the profile picture which allows the abuse management team to quickly view both the sender and the subject of the report. Following the abuse management team's assessment of the report, users who are found to be in breach of the Terms are either issued a conduct warning or have their accounts deleted depending on the severity of the breach. Users are also able to flag inappropriate content in the same way, by clicking on the link which appears between every photo and video.

Bebo also recognizes the importance of working with law enforcement. We actively engage with the relevant enforcement authorities (including the UK Home Office's Single Point of Contact training program) to educate investigators about how to lawfully obtain data from Bebo.

Bebo has a distinct route to report suspected pedophile behavior. This includes critical education material designed to help those unsure about whether the behaviors with which they are concerned constitute pedophilic behaviors. Reports received through this route are dealt with as high priority and reports are disseminated to the appropriate law enforcement agency.

AOL

AOL has a longstanding commitment to safety across the variety of online services that it offers. With respect to child safety, AOL deploys a broad set of technological and policy solutions, including:

- Age-appropriate programming for kids and teens
- Technological solutions
- Monitoring, reporting and enforcement procedures
- Law enforcement cooperation
- Support for public policy
- Safety messaging and education

1. *Age-Appropriate Kids & Teens Programming:*

In its AOL online service, AOL offers age-appropriate content areas for kids and teens. Kids Online services children 12 and under, while beRED is designed for teens between 13-17 years old. AOL uses industry ratings to program these areas with age-appropriate music, movie clips and video games and other content. Programming and advertising in the Kids Online and beRED areas are approved for use by our Policy and Regulatory team.

2. *Technological Solutions*

Parental Controls: AOL has a long history of providing children and families with a safer online experience. More than a decade ago, AOL introduced Parental Controls to help prevent children from accessing undesirable or inappropriate content. We continue to update and enhance our Parental Control software to stay current with changes in technology and online features. Parental Controls are available free on the Web at parentalcontrols.aol.com.

Key features of AOL's Parental Controls include:

- a. Pre-Set Age Controls for Web Browsing: we make the set up process easy by offering pre-set age ranges such as Kids (12 and under), Young Teen (13-15) Mature Teen (16-17) to automatically align Web filtering and monitoring settings to provide an age-appropriate online experience.
- b. Parental Flexibility: When a child tries to access a Web site that is blocked by Web browsing, Parental Controls offers a "Get Permission Now" button which lets the parent approve immediately. If the parent is not close by, the child can send an email to his or her parent for approval. The email Web request shows the name of the Web site and provides the ability to immediately approve or deny access directly from the email.
- c. IM and Email Controls: Parents can know a child's online friends by setting approved IM and email contacts.
- d. Time Limits: Parents can manage a child's Internet time allowing access to the Internet during specified times.
- e. Activity Reports: Parents can choose to view a child's Internet activity online or have a daily or weekly activity reports sent automatically to their email.

SafeSearch: We provide a default SafeSearch feature on AOL Search (search.aol.com). This feature automatically filters out sites with explicit content so consumers can get accurate, reliable results with fewer worries about stumbling across any of the "questionable" material on the Web. Users can customize their filter level at search.aol.com/aol/settings or remove the feature all together.

Screening for Child Pornography: AOL has implemented technologies to identify and remove images of child pornography and to help eliminate the sending of known child pornography. The process creates unique digital signatures from apparent pornographic images and then uses the signature to eliminate further dissemination of the image. We maintain a library of the signatures. When we identify the transmission of one of the images, the transmission is blocked and the image and user information is referred to the National Center for Missing and Exploited Children (NCMEC) for investigation. This procedure provides law enforcement with vital information necessary in prosecuting purveyors of child pornography. Our approach has now become part of a broader cooperative industry effort to remove these images.

Privacy Protections for Communications Tools: AOL offers privacy-related settings within products such as email and instant messaging that enable consumers to control their own online experience by determining who can interact with them:

AIM/AOL instant messaging users have the option to:

- a. Allow all users: Any AOL or AIM user can see that the customer is online and can send them instant messages
- b. Allow only users on the customer's Buddy List: Only people whose screen names the customer has added to the Buddy List® window can see that the customer is online and send them instant messages.
- c. Custom Allow List: Only the people whose screen names the customer has added to the list can see that that the customer is online and send instant messages.
- d. Block all users: No one can see that the customer is online or send them instant messages.
- e. Custom Block List: Only the people whose screen names the customer has added to the list will be prevented from seeing that the customer is online and from sending them instant messages.

E-mail users have the option to:

- a. Allow mail from all senders
- b. Allow mail from Bebo and associated AOL domains only
- c. Allow mail only from people the customer knows.
- d. Block mail from all senders.
- e. Custom: Allow and/or block only people whose email addresses the customer adds to the list.
- f. Block email containing pictures and files

3. *Monitoring, Reporting and Enforcement*

Report Abuse: AOL-branded services offer a prominent and convenient "Report Abuse" button for consumers to report unacceptable behavior that they encounter on our network. Our Report Abuse mechanism automatically captures text of IM and chat conversations so that they are authenticated and cannot be manipulated prior to sending the report.

The information is referred to teams of trained professionals who process consumer complaints on a 24x7 basis. The team is trained to handle images of child pornography and text-based child solicitations as well as:

- a. Hate speech
- b. Harassment/cyberbullying
- c. Self-harm
- d. Reckless behavior of minors
- e. Sexually-explicit material

4. *Law Enforcement Support*

Law Enforcement Training: AOL works to train law enforcement personnel in venues across the United States. In 2007, AOL delivered state-of-the-art technology and forensic training to the National District Attorneys Association; the National Association

of Attorneys General; the National Child Advocacy Center; the American Prosecutors Research Institute; the Naval Justice School; several Internet Crimes Against Children regional task forces; the Federal Energy Regulatory Commission; and 14 separate audiences of law enforcement investigators and prosecutors at the National Center for Missing and Exploited Children.

Law Enforcement Support: AOL assists law enforcement on thousands of cases per year. Through support services, such as our 24-hour dedicated law enforcement hotline, our team responds to law enforcement requests, answers officers' questions about what types of information would help their cases, and provides guidance on obtaining the right information. Litigation Support: Since 1995, we have offered pre-trial litigation support, as well as fact and expert witness testimony on criminal cases involving records obtained from AOL services. In 2007 AOL testified in approximately one dozen criminal cases throughout the United States, in the role of "custodian of records" and, in more complex cases, in the dual role of fact and expert witness on AOL technologies and procedures.

Amber Alerts: AOL was the first ISP to initiate an AMBER Alert program by which our customers can receive e-mail and IM alerts targeted to their area.

5. *Support for Safety-related Public Policies*

AOL has worked closely with legislators and others in industry to develop and support child protection legislative initiatives throughout the States including; laws to prohibit online enticement of minors and Internet safety curricula requirements, as well as legislation to improved data preservation, prevent cyberbullying and strengthen enforcement. .

6. *Safety Messaging and Education*

AOL recognizes that education is one of the most effective ways to help protect against child predation. In our continuing effort to teach online safety we:

- a. Built SafetyClicks.com, a safety blog that features articles, videos, and topical blog posts designed to support and inform parents as they teach their kids to navigate in the Internet.
- b. Offer safety tips to kids and parents at the product level (such as on AOL's Kids' Message Boards).
- c. Provide child online safety education in the form of formal presentations or hands on demonstrations at schools, PTA or other organized meetings.
- d. Work with a myriad of Child Advocacy Organizations to help educate kids, parents and caregivers about safe Internet use.

What results can you share about the actual impact of your various efforts in #2 to date? Please be as specific and data-driven as possible. What lessons have you

learned from your efforts to execute in #2? If any of your approaches have not been as successful as you hoped or have had unexpected consequences, please provide a detailed case study.

We measure the success of these programs by looking at:

1. Decreases in Events: The reduction in child endangerment events reported on our service.
2. Law Enforcement Participation: The number of law enforcement training sessions conducted by AOL.
3. NCMEC success: The number of arrests and convictions made from AOL graphic and text-based reports sent to NCMEC.
4. User Monitoring: The number of legitimate abuse reports submitted by our users.
5. Parental Controls: The number of parents using Parental Control tools.
6. Technology Adaptation: The number of outside Internet services adapting AOL's or similar child protection technologies.

What can you share about any efforts you are planning to launch in the future? Please describe in as much detail as possible. What problem are you trying to solve with the additional efforts and how will you measure success?

University Alerts: In response to the tragedy at Virginia Tech, AOL embarked on a project to make alerts available to colleges and universities. Through this program, colleges and universities can send emergency notifications to through email, IM and text messaging to students, faculty, employees, and other interested persons. The program is currently in the pilot stage at Shenandoah University in Virginia.

New Content Standards: Bebo recently finished a review of its commercial content standards policy to validate that it is consistent with Bebo's commitment to offering its audience an appropriate social networking experience. Bebo has also taken recognized rating systems and industry self-regulatory codes of conduct into consideration. Bebo's new standards will help our partners better identify prohibited content; content that needs to be age-restricted; and content that requires a guidance label. Additionally, Bebo will soon provide its partners with the ability to age-restrict and label their content at the point they uploading this material.

Based on what you've learned in trying to execute safety measures, what should the Technical Advisory Board know about dealing with actual implementation issues?

Bebo and AOL would like to re-iterate our belief that there is no single "solution" to online child predation - and that only a multi-faceted approach is likely to succeed in minimizing the risk of harm to young people.

Furthermore, we believe that parental involvement cannot be mandated. AOL and Bebo provide parents a broad variety of tools and controls designed to help them protect their children online, as well as a steady stream of safety tips and other safety information. Despite these efforts, however, there are still a large number of parents who neglect to participate in the online experience of their children. This suggests that education must continue to be a focus.

There are, however, some clear bright spots. We have found that the “Neighborhood Watch” concept is effective. Asking users to report inappropriate material that they encounter serves as a powerful tool in effectively policing products and services. Users want a clean environment and are happy to report bad actors as long as they see action taken when they report.

We have learned that education is an effective means to protect children. To that end, we actively work with the education sector and supply them with the tools, knowledge and skills they need to educate young people to use the internet safely and responsibly.

We have also learned that online communities can be a tremendous force for good. To compensate for a range of support deficits that may exist in a young person’s life, Bebo has worked with mental health and social care support organizations to ensure that its users have ready access to sources of expert advice and support from within the online community they inhabit. This can result in a number of positive outcomes, not least of which is that access to support and advice online can normalize help-seeking as well as de-stigmatize issues like mental health, poor body image and concerns about family relationships. These are precisely the vulnerabilities that predators leverage when soliciting young people online.

What concerns do you have based on your own experiences?

We have learned that a “silver bullet” cure the dangers of the Internet does not exist. The safety challenges online are remarkably complicated, and moving forward we need to keep in mind the fact that:

1. The line between moderating and censoring becomes more challenging in the Web 2.0 world.
2. Context is relevant. What is ok to say in one kind of forum is not ok to say in another kind of forum
3. Restricting minors from popular content and services without viable, age-appropriate alternatives may push them to mature areas that they do not belong.
4. Implementing technological solutions often fosters a game of cat and mouse. Determined users can often find ways around technical safeguards.

What are the strengths and weaknesses of implementing technical solutions?

Strengths:

1. Automates the processing of vast quantities of information rapidly and intelligently.
2. Reduction of human error.
3. Results can inform programmers of research the findings of which augments understanding of patterns and processes of both use and misuse of a service.
4. Constant moderation and review.
5. Scalability with minimum increase in resources.
6. Self-correcting results – parameters can be re-calibrated as knowledge base grows.

Weakness:

1. Keeping technology up to date with current trends and issues.
2. Lack of nuance that can lead to over-broad application (for example, the contexts in which words and phrases are used are as important as the word or phrase at issue).
3. Technologies can be gamed.
4. Technologies are not consistent over platforms.



COMMUNITY CONNECT INC.

Statement to the Technical Advisory Board from Community Connect, Inc.

Contact:

Bernadette Sweeney

Member Safety Initiatives 2008

Community Connect, Inc. is the parent company of five social networking sites including BlackPlanet.com, MiGente.com, AsianAve.com, FaithBase.com and GLEE.com. BlackPlanet.com is our largest site and it is also the largest online community for African Americans.

Members use our sites to reconnect with old friends, meet new ones and visit the site daily to create relationships and exchange information while creating trusted networks between themselves. Our sites are embraced by celebrities and key personalities who are relevant to the audience and want to connect with them. We have high loyalty among our members because of our culturally relevant material focused on our member's backgrounds and interests.

We are committed to providing a safe environment for all our members across all our sites. Therefore, we have developed a comprehensive member safety campaign to help educate our members about how to have a fun and safe user experience. Our Member Safety initiatives focus on two key areas, unwanted content and unwanted contact. Our belief is that all members will have a safer online experience if they can control who can contact them and if the content they are exposed to does not violate any of our Terms of Service.

Our member safety campaign falls into four categories:

1. General Member Safety
2. Controlling Contact From Other members
3. Under 18 Member Safety
4. Education and Partnership With External Organizations



1. General Member Safety Targeting Members of All Ages

- We have updated the Terms of Service to reflect the current state of the internet and to include online safety tips for teens, parents, daters and law enforcement agencies.
- We created and posted an email address for concerned parents and law enforcement agents to easily contact us with any issues or concerns.
- We prominently display “Report Abuse” links everywhere there is member to member communication.
- We have added a photo approval process for all social main photos to prevent inappropriate photos from appearing as the main photo on personal pages. This photo approval process is outsourced to a third party.
- Members can control Member Find results so that only people in their age range are displayed in search results.
- All main photos in Groups require approval. This was implemented in March 2008. This approval process is outsourced to a third party.
- We have created a tool that prevents members from creating and searching for forums or groups using words that have been banned by the Member Safety Team. Examples of banned words include child porn and pornography.
- Safety Tips contain resources for Internet Safety including FTC tips.
- Phishing warnings are contained in Safety Tips.
- Users must affirm they have read the Safety Tips prior to registration.
- We have a team of moderators trained to investigate and respond to all member reports of member safety violations.



COMMUNITY CONNECT INC.

2. Controlling Contact From Other Members

We know that our members have different comfort levels about how much personal information they want to share with other members. We want every member to be able to decide how much or how little information they want to reveal about themselves.

Members have options and can select how much information they want to share with others.

- Members can opt to make their profile viewable to “Friends Only.”
- Members have the ability to block all or some members from sending notes and friend invites based on age, gender, relationship status and sexual orientation.
- Members can opt not to allow other members to IM them.
- Members can opt not to allow themselves to be searched by their real name, email address and location.
- Members can block individuals from contacting them using notes and IM.
- Members can choose not to display their age, name, sexual preference, their last log in date, how long they have been a member, race, education and income.
- Members can hide their online status so other members can not tell if they are online.



3. Under 18 Member Safety and Education

We are committed to providing a safe environment to all our members especially members between the ages of 14-18. These members may not have a lot of experience navigating cyberspace so we have extra measures in place to help them safely navigate through our site.

- We created a special welcome email for members between the ages of 14 and 18 to provide a site overview and a reminder about internet safety with a link to online safety tips.
- We added age restrictions to chat rooms to prevent members under 18 from entering certain rooms and members over 18 from entering the teen chat rooms.
- After registration, we automatically add a friend to all members who are between the ages of 14-18. The friend, from Member Services, will regularly post notices on their bulletin board reminding members how to stay safe online.
- Members can not change their date of birth after registering.
- We changed the registration process to make it more difficult for a person under the age of 14 to lie about their age to become a site member.
- Safety Tips for Parents includes a suggestion to consider using computer based blocking software.
- The default setting for members under 18 is set to “Do not send notes to me from anyone over 18.”
- We added age restrictions to Groups. If a member under 18 creates a group, members over 18 can not join and vice versa.
- Members under 18 can not hide their age.
- We recognize that members who are between 14-18 are minors and we do not show them ads for alcohol or other ads designed for more mature audiences.



4. Partnerships With External Organizations

Our members are extremely important to us and as a commitment to them we have joined with government agencies, organizations, and other social networking sites to comprehensively address member safety.

Partnership with New Jersey Attorney General's Office

- In October, 2007, we entered into a partnership with the New Jersey Attorney General's Office and other social networking sites to develop an icon that will empower users by allowing them to quickly and easily report inappropriate content or suspicious activity. Because the icon is uniform, all users have a clear idea what it means and will thus be able to quickly report abuse.
- In addition to developing a standard icon, the sites and the Attorney General have also worked together to develop consistency with respect to what occurs after the icon is clicked.

Partnership with Online Safety Organizations

- We have supported and worked with several non profit organizations that are tasked with increasing online safety and education including www.wiredsafety.org, the largest and oldest online safety organization and www.safefamilies.org, an online organization who's mission is to teach parents how to help keep their children online.
- We have links to both organizations in our Safety Tips section.
- In January, 2008, Bernadette Sweeney, the Director of Member Services at Community Connect, was given the honor of becoming an honorary Teen angel. Teenangels is a group of 13-18 year-old volunteers that have been specially trained by the local law enforcement, and many other leading safety experts in all aspects of online safety, privacy, and security. After completion of the required training, the Teenangels run unique programs in schools to spread the word about responsible and safe surfing to other teens and younger kids, parents, and teachers.
- Honorary Teen Angels are selected because of their commitment to teenage online safety.



COMMUNITY CONNECT INC.

The steps we have taken to help increase member safety and awareness have all been developed in house and most of the initiatives are managed by an internal team of Member Services Moderators. The photo approval tool was developed in house and is managed by an outsourced team of moderators.

Our tools were designed to measure how many members have opted to use the safety features we have in place. We can track how many emails we receive to the member safety address; we can track how many members click on our safety tips and our safety messages; we can track how many members use the Report Abuse link to report Terms of Services violations and we can track how many members opt in to use the privacy settings available to them and which ones are being used the most.

We are confident that the overall impact these initiatives have had on member safety is positive. However, we do not think it is fair to attach a number to member safety. For example, no one should assume that if 80% of members of any social networking site are using one or more privacy settings then 80% of members will be safe online. This assumption can not and should not be made. We will not stop researching and building new tools for increasing online safety just because a majority of our members are using all or some of our existing safety tools.

We are confident the initiatives in place thus far have had a positive impact on member safety. However, there is one activity that concerns us. Our initiatives to date have not been able to fully eradicate member behavior that is acceptable on the peer to peer level but still violates our terms of service. For example, a member may willingly post his or her address, phone number and school onto his or her personal page. Other members may willingly upload photos containing nudity and set the status to "Friends Only" meaning all members who are approved friends can see the photo. Both the sender and the receiver are willing participants in uploading and viewing "bad" content.

Peer to peer "bad" behavior is an area where we would like to have further discussion with the task force and other social networking sites. We strongly believe there is a need to educate our younger members about what should and should not be uploaded onto any website. We welcome any feedback and suggestions from the TAB and the other Social Networking Sites that are part of the task force team to help address this issue.



COMMUNITY CONNECT INC.

BlackPlanet has the power to communicate with millions of members. We understand that with power comes great responsibility. While we will continue to research and implement technical solutions that work for us and our members we also want to use our reach to continue to educate our members. We are committed to partnering with organizations and groups that are dedicated to educating teenagers and adults about online safety.

In 2009, we will focus on creating a cyberbullying awareness campaign for our members. This campaign will target our members in the 14-18 year age range. We plan to create in house Public Safety Announcements that will be posted throughout the site. Our goal is to create awareness about the issue and to make our members understand that certain behaviors are should never be tolerated even if it a "Friend" who is initiating an unwanted action or behavior.

We also plan to add another option to the privacy settings. Our product roadmap for 2009 includes adding the option to allow members to block other members from visiting their page based on age range. As an example, members will be able to tell us not to let members between 18 and 25 view their page.

When this is implemented, the default setting for members under 18 will be to not let anyone over 18 view their page.

We have an ongoing commitment to member safety and we will keep seeking solutions that help educate our members and help them prevent unwanted content and contact. We want to clearly state that we are not against implementing technical solutions if they can add value to our community by providing a safer online environment.

The technical presentations shown at the Task Force meeting in September offered various methods and tools that were deemed by their presenters to help create a safer online environment. However, based on the questions and concerns that followed each presenter, none of the presentations offered a magic bullet solution that guarantees online safety.

When making recommendations we strongly encourage the TAB team to consider the effect that some of these technologies would have on the site members and the business itself.



COMMUNITY CONNECT INC.

Implementation and cost alone may be prohibiting factors for smaller social networking sites. MySpace and FaceBook may be able to easily absorb the additional costs associates with implementation. However, smaller, niche sites, like ours, may find it impossible to meet the challenge of implementing new software and the increased costs involved. We are very concerned about any associated cost that may be incurred if any of the technologies presented were mandated.

Again, we are not against exploring technology that can help improve online safety. However, none of the solutions addressed bigger issues such as cyberbullying and other “peer to peer” bad behavior. None of the “solutions” presented at the Task Force meeting had answers that addressed these very important issues.

We strongly believe that technology alone can not and will not provide an absolute safe online environment. Education of the parent and child needs to be part of any online safety equation.

We are impressed by the dedication to online safety that everyone on this task force has shown. We would like to continue to move forward to address this issue and hope that we can work with the other members of the task force to come up with shared solutions and best practices to educate and help keep all members safe online.

Company Overview:

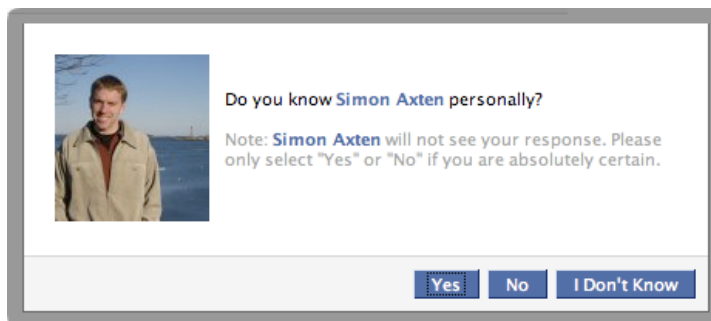
Facebook is a social utility that gives people the power to share and makes the world more open and connected. The site has over 100 million active users from around the world, and more than 50 million people use Facebook every day.

Relevant URLs: www.facebook.com
 www.facebook.com/privacy
 www.facebook.com/help.php

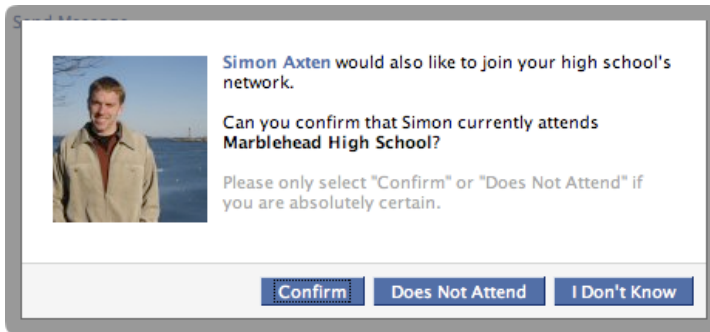
1. The principal safety issue Facebook works to address is anonymity. While appropriate in some settings, fake names and hidden identities are incongruous with Facebook's goal of allowing people to share and communicate more openly and efficiently. When users are allowed to misrepresent themselves, trust and accountability break down, and people feel less confident in their interactions. Bad actors are emboldened because there is little chance of serious consequence. Most of the systems and processes we have developed are intended to solve this root problem, and we measure the risk that youth face on our site by how well we are doing in this effort.
2. Facebook's network-based architecture strives to reflect as closely as possible real world social communities. By default, users' profiles are only available to those who share networks with them or have been confirmed as friends.

We provide extensive and particular privacy controls that allow users to specify what information they make available and to whom. Users can restrict access to their profile to confirmed friends only, and can even create lists of people from their larger friend group to tailor privacy further.

Facebook employs a system of peer verification for users who identify themselves as under 18. This system relies on answers to questions accompanying friend requests to help determine if the user sending those requests attends a particular high school or knows the people he or she is contacting. Accounts are either verified or disabled based on these answers.



A high school network affiliation must be established through the process above before a user can gain access to the profiles of others on that network. Users must be 18 or under to join a high school network.



Regional networks are segmented by age. By default, minors cannot see the profiles of adults on the same regional network, and vice versa. Adults also cannot browse for minors based on profile attributes.

Users can report suspicious content or behavior using the report links located throughout the site. They can also use the contact forms on our Help page or send an email directly to one of our several aliases, which include info@facebook.com, privacy@facebook.com, and abuse@facebook.com.



We are committed to reviewing all user reports of nudity, pornography, and harassing messages within 24 hours and resolving all email complaints sent to abuse@facebook.com within 72 hours.

We have developed several automated systems to detect anomalous behavior and block or disable the accounts of potential bad actors. Obviously, we must keep the signals these systems use confidential, but they generally look for unusual patterns in activity, and interactions between non-friends are looked at much more closely than those between friends. Some examples of things these systems look for are users whose friend requests are ignored at a high rate, or users who are contacting lots of people not on their friends list. They also look for adult users who are contacting an inordinate number of minors.

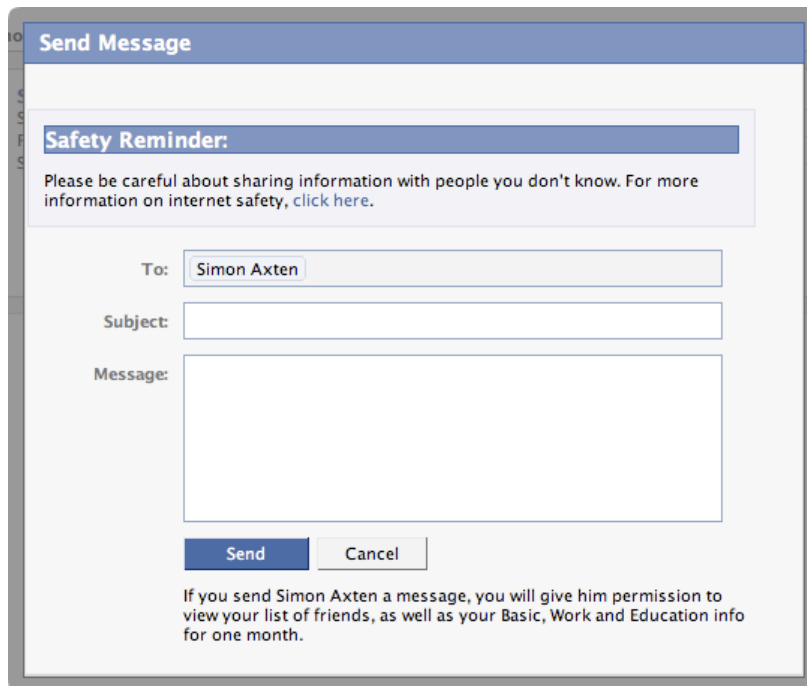
People who try to sign up with a birth date that makes them under 13 are blocked, and a persistent browser cookie is used to prevent further attempts at sign-up.

Users cannot edit their birth date to one that makes them under 18 without first contacting our User Operations team for review.

Facebook maintains an extensive blacklist of words likely to be associated with fake accounts, which is then used to block these accounts at sign-up.

Users cannot change their names without first submitting the change for approval. This is done through an algorithm that uses our blacklist and other factors to identify likely fake names.

Users under the age of 18 are shown a safety reminder any time they receive a message from, or begin composing a message to, an adult user with whom they have no mutual friends. This reminder tells them to be careful when sharing information with people they do not know, and provides a link to Facebook's Safety page.



The image shows a screenshot of a Facebook 'Send Message' dialog box. At the top, there is a blue header with the text 'Send Message'. Below this, a white box with a blue header contains the text 'Safety Reminder:'. Underneath, a message reads: 'Please be careful about sharing information with people you don't know. For more information on internet safety, [click here](#).' Below the reminder, there are three input fields: 'To:' with the name 'Simon Axten' entered, 'Subject:', and 'Message:'. At the bottom of the dialog, there are two buttons: 'Send' and 'Cancel'. Below the buttons, a small disclaimer states: 'If you send Simon Axten a message, you will give him permission to view your list of friends, as well as your Basic, Work and Education info for one month.'

Facebook has developed several automated systems to detect and disable fake accounts based on anomalous behavior, and is constantly working to improve these.

We disable the accounts of convicted sex offenders and work closely with law enforcement in cases where a minor has been contacted inappropriately, or where a user has committed a crime. We also plan to add the KIDS Act registry to our many existing safeguards and to use the database as vigorously and comprehensively as we can. Specifically, we will check new users at sign-up and review existing users as regularly as the technology allows. Anyone on the list will be prevented from joining Facebook. Anyone already on Facebook who is added to the list will have his or her account disabled. We will also continue to enhance our partnership with law enforcement to find and prosecute sexual predators who violate this new law with fake names, addresses, or handles.

We are working with Attorney General Milgram of New Jersey to test a different version of our report link in order to see what effect it has on the volume and quality of reports. We have also been working closely with Attorney General Cuomo of New York and Kroll, our independent safety and security examiner, on safety issues.

All of the above efforts are in-house. Facebook employs a team of User Operations analysts to resolve user reports and respond to complaints, as well as team of Site Integrity engineers to develop and fine-tune our automated systems.

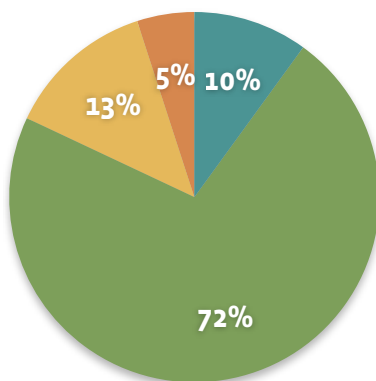
We are deeply committed to our own efforts in this area and believe the controls and processes we have built are leading the industry. At the same time, we recognize that protecting children online is an ongoing battle that requires cooperation among various groups, and we are always open to working with outside companies that have developed smart solutions.

- Facebook tracks data on all of its automated systems, as well as on reports and complaints we receive from users and the actions we take on them. While we cannot provide specific numbers, we do receive hundreds of thousands of contacts each week. These include reports of nudity, pornography, and harassing messages, which we resolve within 24 hours. Our 100 million active users take great pride in keeping the site clean and are quick to report content and behavior they find offensive or threatening. Our quick response time in dealing with these reports has kept dangerous users off the site, and the very low number of serious incidents involving adults and minors who have met through Facebook is a testament to this.

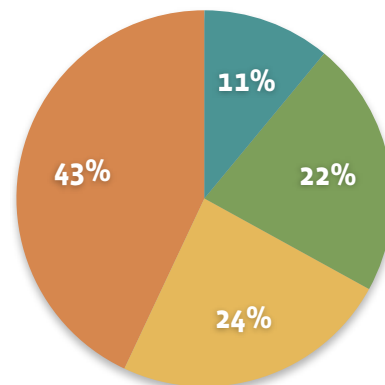
We have also used our own Polling feature to gauge how minors are using the site, as well as how safe they feel on Facebook relative to other sites and the Internet at large. The results of a few of these polls, which use a sample of 500 users in the US aged 13-17, are below:

Have you ever seen nudity...

...on Facebook?



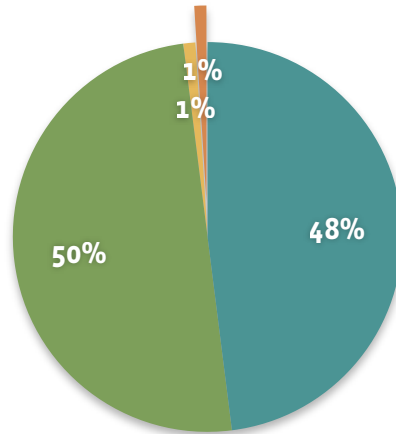
...on a website other than Facebook?



Green – No, never.
Yellow – Yes, a few times.
Orange – Yes, more than a few times.
Blue – I don't know.

These results show how effective our systems and processes are at keeping bad content off the site. Teens are much less likely to encounter nudity on Facebook than they are elsewhere on the Internet.

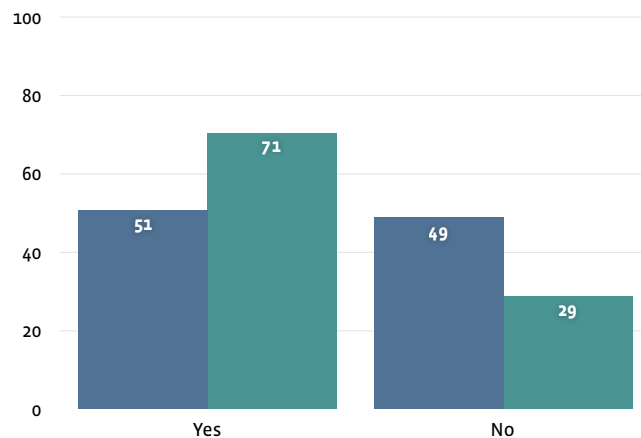
Do you know the people you interact with on Facebook in real life?



Green – Yes, most of them.
Blue – Yes, all of them.
Yellow – No, only a few of them.
Orange – No, none of them.

This poll shows that the vast majority of teens are using Facebook to communicate with people they already know in the real world. Because they are conditioned to use the site in this way, they are less likely to engage with a stranger on Facebook who might do them harm.

Have you ever used Facebook's privacy settings to limit access to your information?



Blue – Male
Green – Female

In fact, 100% of teens use our privacy controls because of the defaults we have put in place. This poll shows that 63% edit their settings even further, with girls using these controls slightly more often than boys.

In working to keep kids safe on Facebook, we have learned that technical solutions are imperfect, and that systems must be evaluated and refined on a regular basis to remain effective.

On the one hand, these systems must be focused enough not to produce a high rate of false positives. Controls meant to protect people will inevitably block some legitimate behavior. Our name blacklist, for example, prevents people with unusual names, or names shared by celebrities or other public figures, from signing up. These people must contact our User Operations team and prove their identity in order to create an account on the site. Likewise, our various systems for detecting anomalous behavior occasionally block or disable the accounts of people who are using the site in benign, but unanticipated and perhaps unintended, ways. The key is to establish an acceptable threshold for misses and then use these to inform and improve systems where possible. Because Facebook is a utility for sharing and communicating more efficiently, we must be careful not to restrict the power of the tool any more than is necessary to protect our users.

On the other hand, real bad actors are creative, and they quickly adapt and develop new methods when controls are built to block them. Facebook works hard to anticipate these changes and to quickly identify new dangerous behavior so that it can be stopped.

4. Unfortunately, we cannot provide specific details about our plans for the future. More generally, though, Facebook's mission, as well as our values of authenticity and control, will continue to guide the product. We will continue to develop and refine systems that discourage interactions between strangers, and encourage those between people who know each other in the real world. We are particularly focused on developing new ways to identify fake accounts and suspicious behavior, which will help us maintain the integrity of the social graph while improving safety and protecting our users from annoying phishing and spam attacks. As mentioned above, Facebook has been a strong supporter of the recently passed KIDS Act, and we plan to use the registry it creates to keep sexual predators off Facebook.
5. Once again, we have learned from experience that technical solutions, while helpful, are imperfect and must be accompanied by education and manual processes in order to truly be effective. Facebook has taken a multi-faceted approach to the problem of protecting kids online, using automated systems where they make sense, but also educating users on safe practices and staffing a responsible team to quickly review and respond to serious reports of misconduct. We have consistently found that blunt, heavy-handed approaches are the least effective, as they prevent legitimate use of the tool or service and provide bad actors with numerous options for circumventing controls.

Instead, Facebook recommends smarter, more focused systems that aim to block dangerous behavior while disrupting legitimate communication as little as possible. That being said, the very nature of the problem requires constant evaluation and refinement of these systems, as the behavior of both legitimate and bad actors can change over time. We believe that technical solutions should be focused primarily on the use of false identities and communication between people who do not know each other in the real world.



Orkut is Google's online social network. It is particularly popular in Brazil and India. Google takes the safety of our users on orkut very seriously, and we have gone to great lengths to help protect them. Unlike many other social network sites, orkut requires users to be 18 years old to use the service. Google places a session cookie on a registrant's browser to help prevent age falsification when a user registers for orkut. Therefore, many of the issues related to the safety of young people under 18 on social networking sites do not generally apply to orkut.

Google/orkut focuses its safety efforts on combating inappropriate content on orkut. We have a cross-functional team of product managers, engineers, legal and customer support employees across three continents who are dedicated to developing abuse-prevention tools for orkut. This team has a three-pronged approach to detecting and preventing abuse on the website:

- Identifying and removing illegal content
- Empowering users to detect and prevent abuse
- Cooperating with law enforcement

Identifying and Removing Illegal Content:

Orkut uses cutting edge technology and manual content reviews in response to user "flags" to qualify "manual content reviews" to identify and eliminate illegal and inappropriate content from orkut. From a technological perspective Google uses the following tools:

- *Image scanning technology:* This year we launched image scanning technology which aims to detect images of pornography (including child pornography) at the time of upload to the website, followed quickly by removal. A team of U.S. engineers worked on development of this scanning technology for more than a year, and we are very pleased with the results of the tool's detection capabilities thus far.
- *Spam detection technology:* And our orkut engineering team in India developed significant improvements to our spam detection technology in the last year, vastly reducing the amount of spam that appears in users' scrapbooks and elsewhere on the website.

These safety tools complement an extensive manual content review process in response to user flags. Our operational orkut support team conducts manual content reviews each day of content flagged by users. Google has worked very hard to develop and improve these internal systems for detecting and preventing illegal content from appearing on the website. Our manual review process works as follows:

1. First, the user uploads new content.
2. If content is flagged by users of the website, that content is queued for review.
3. If our image scanning technology detects inappropriate content, that content is automatically removed from the website.
4. Our manual reviewers will review the content flagged for review by users, and will remove content that violates the site's Terms of Service or Community Standards.
5. If the manual reviewer identifies pornographic images not already detected by our image scanning technology, the reviewer provides relevant information to the image scanning database to identify duplicate images automatically in the future.

Empowering Users to Detect and Prevent Abuse

Google empowers users to contribute to keeping orkut free of inappropriate content and has developed a number of tools for users to assist us in this goal.

For years, the orkut website has had a Report Abuse button on every profile and community page on the website. In the past year, the engineering and support teams also have added this button to photo albums and other pages so users can now flag more specific items for review.

1. When a user clicks on the Report Abuse button to report a profile or community, the user is taken to a page that asks the user to identify the category of inappropriate content at issue.
2. If a user clicks on any of those buttons, the user may be taken to another page to provide even more details about their report.
3. On the backend, our engineers have developed a detailed system for queue-ing up reports from these flags in an order most likely to bring the gravest concerns to the top of queue, so that our reviewers will be able to see and remove the most egregious of the flagged content first.
4. For photo albums, our engineering and support teams have created a slightly different version of the reporting page, giving users an opportunity to describe their complaint in more detail. Often, such descriptions from our users are vital for our support team to determine whether non-pornographic photographs violate our Terms of Service.

In addition to giving our users sufficient tools to report inappropriate content to us, we also feel it is important to provide educational resources for our users, including safety tips, and explanations of what type of content is not allowed on the site. We do this in our Safety Center, which is available via a link that appears in the footer of every single page of the orkut website.

The Safety Center includes the following resources:

- links to orkut website policies, such as the Terms of Service and the Community Standards
- detailed descriptions of our privacy and security features
- links to third-party resources, such as non-governmental organizations that focus on Internet safety

Working with law enforcement

Two summers ago, we realized that the community flagging and reporting abuse tools and safety center tools were not sufficient for law enforcement to communicate with us. When law enforcement has concerns about content on the website, we want to ensure that we hear their concerns first and prioritize their removal requests above all others.

To that end, in Summer 2006 our U.S. engineers created a special Priority Reporting Tool for the exclusive use of law enforcement. This tool is now used by dozens of law enforcement agencies across Brazil and India, and has been a highly effective means of communication between our support team and the police. We hope to work with law enforcement in the United States to use this tool in a similar way.

Through this tool, law enforcement flags of inappropriate content go straight to the top of our queue, and we promise a 1-business-day turnaround in reviewing and responding to those flags. The tool also allows law enforcement the opportunity to request preservation of the user data associated with the flagged content, ensuring that if law enforcement later seeks a court order for such information, we will have it available for them.

The orkut support and legal teams have found this tool to be tremendously effective in streamlining and prioritizing the needs of law enforcement with regard to content on orkut.

In the U.S., we also report all illegal images of child pornography that we discover on the website to the National Center for Missing and Exploited Children, as required by U.S. law.

October 17, 2008

Re: Internet Technical Safety Task Force Submission

To Whom It May Concern:

Loopt is a proud member of the Internet Technical Safety Task Force. It has been an honor to participate in this undertaking with our industry colleagues, the several online safety and privacy non-governmental organizations involved, and the entire Berkman Center team including the technical and research advisory boards.

Of particular note were the presentations of the Research Advisory Board during the April 30, 2008 meeting, which were profound and extremely valuable in terms of helping us all move forward in an effective manner to address these issues. Amanda Lenhart (Pew Internet & American Life Project), Janis Wolak (Crimes against Children Research Center), Michele Ybarra (Internet Solutions for Kids, Inc.), and dana boyd (Fellow, Berkman Center for Internet and Society) presented in-depth studies and research that shed light on the complex problems and behaviors intertwined under the umbrella of 'online safety'.

We have learned a significant amount through this process and know that the proceedings over the past year will most definitely result in raising the caliber of online safety solutions. It is clear that industry continues to invest significant resources to address these issues. Loopt has benefited from collaboration with industry peers such as Fox Interactive, Microsoft, Xanga, Facebook, AOL, Linden Lab, Verizon, and AT&T. In addition, the contributions and input of the various online safety and privacy advocacy groups have been invaluable, including Connect Safely, Progress & Freedom Foundation, Center for Democracy & Technology, Enough is Enough, WiredSafety, and Family Online Safety Institute.

We would like to thank MySpace (Fox Interactive) and the 49 State Attorneys General for putting together this group, as well as the Berkman Center team for deftly handling the process. Finally, we hope that the members of this task force will consider continuing our work together in a similar manner into the next year and beyond.

Sincerely,

Brian R. Knapp
Vice President, Corporate Affairs
Chief Privacy Officer

ABOUT LOOPT. Loopt is based in Silicon Valley and backed by leading venture capital firms, Sequoia Capital and New Enterprise Associates. Loopt has created an interoperable and accessible "social mapping" service that is available across multiple carrier networks and supported on over 100 mobile devices. Loopt shows users where their friends are and what they are doing via detailed, interactive maps on their mobile phones. Loopt helps friends connect on the fly and navigate their social lives by orienting them to people, places and events around them. Users can also share geo-tagged photos and comments with friends in their mobile address book or online in social networks, communities and blogs. Loopt was designed with user privacy at its core and offers a variety of effective and intuitive privacy controls. www.loopt.com

I. OPT-IN, PRIVACY CONTROLS.

Opt-in Consent. Loopt is 100% permission-based; express, informed opt-in consent is received from every subscriber. Each subscriber must proceed through a multi-step registration process, during which they are presented with key information about the service and several ways to review Loopt's end user agreements.

Mobile phone number-based Accounts. Every Loopt account is tied to a single, valid and authenticated mobile phone number, which number cannot be later modified for that particular account or device.

Notification Program. Following registration, an automated "reminder" notification program reminds users that Loopt is now installed on their mobile device, and contains key messages about using the service responsibly. These notifications are delivered at random intervals via SMS (short message service) or device-based push notification during the first ten days following registration.

Closed Networks. Loopt subscribers only share exact location on the Loopt Friends Map with established friends. To initiate a friend request, a subscriber must already know the other user's mobile phone number. Even when a Loopt friendship request is successfully delivered, the prospective friend must consent to a *reciprocal* "friendship connection" before any map-based location sharing will occur.

Privacy Controls. Loopt offers several intuitive, powerful and effective end user privacy controls.

- *Controlling Loopt Friend Connections.* Subscribers may immediately "hide" from sharing information or "block" profile access on a friend-by-friend basis, or from all Loopt friends at once using the one-step "Hide All" function. In addition, subscribers may delete or terminate friendship connections permanently at any time.

- **Report Abuse.** Report Abuse links are posted near every subscriber profile. Loopt's powerful "Report Abuse" feature, as provided in the Loopt Mix service, offers users the ability remove their profile from future viewing by specific users, and terminates any in-progress messages or communications between the abuse reporter and those reported-users. In addition, Loopt's customer service and privacy-response team reviews all Report Abuse messages and responds appropriately according to internal process standards and Loopt's publicly-posted Terms of Use (available at <https://app.loopt.com/loopt/termsOfUse.aspx>).
- **For Parents.** Parents or guardians may delete their minor child's Loopt account altogether, at any time, by contacting Loopt customer service by phone or email.

Privacy Notice. Loopt's Privacy Notice is readily viewable on mobile devices and online, and may be received by email delivery or postal mail. Loopt is *TRUSTe*® certified. Loopt will not disclose subscriber information to third parties for marketing purposes, unless the particular subscriber has opted-in to be part of a specific program or feature in accordance with the applicable Loopt consent procedures. (Privacy Notice, available at <https://www.loopt.com/loopt/privacyNotice.aspx>)

II. USER EDUCATION, DISCLOSURES.

FAQs, User Agreements. Loopt's end-user agreements (Terms of Use, Privacy Notice) are readily available at the Loopt Web site, within Loopt's mobile application, and can be delivered to users by email or postal mail. In addition, Loopt's Web site contains detailed information about our privacy and security features, as well as Frequently Asked Questions.

Safety, Privacy Tips. Loopt's Web site offers educational "tips" for both subscribers and parents to encourage informed, responsible usage.

User Education. Loopt takes advantage of "teachable moments" during the user experience in order to remind users about responsible and effective usage. For example, prior to permitting the acceptance of any Loopt friendship request, a pop-up notice screen is displayed to remind the user to confirm the legitimacy of the particular friendship-connection request.

III. CUSTOMER SERVICE, COMPLAINTS.

Privacy, Content Complaints. Loopt promptly addresses customer complaints or concerns regarding security, privacy, or content with a well-trained, in-house customer service team. Loopt customer service representatives are trained to anticipate misuse situations and empowered to immediately suspend questionable accounts. Any challenging situations are escalated to Loopt executives and promptly discussed among the operations team.

Terms of Use Violations. Loopt will promptly notify, suspend, or permanently ban users who violate Loopt's community policies and regulations including the posting of inappropriate content or the harassment of other subscribers.

Customer Service. Loopt accepts complaints about harassment, unwelcome contact, and inappropriate content via phone (during normal business hours) and email. Customer service contact information is clearly and prominently highlighted on the Loopt Web site and within the Loopt mobile application.

IV. BACKGROUND TECHNOLOGY.

Mobile Application Security. To prevent “spoofing” of a mobile phone number with the main server during subscriber registration, Loopt verifies the mobile phone number via a background SMS “handshake” with the applicable Loopt mobile application. This “handshake” acts to verify and authenticate that the registering subscriber has custody of that particular handset with the mobile phone number indicated during registration.

Application Time-outs. Loopt automatically logs-out subscribers and puts them into a “disabled” state after certain periods of non-usage are detected by our systems. To reactivate their profile, subscribers must log back into the Loopt mobile application.

Age Limits. Loopt's Terms of Use includes a minimum age requirement, currently set at 14 years of age. Loopt has implemented an “age-neutral” screening mechanism in its subscriber registration flow, which requires – in a neutral fashion – users to input their age and rejects users who do not meet the minimum requirement. Loopt tags the mobile device of such unsuccessful registrants and prevents those prospective members from re-registering from the same device. This screening mechanism works in accordance with the FTC's guidance with regard to COPPA compliance. In addition, parents and guardians may contact Loopt to terminate accounts of underage subscribers.

Background Monitoring. Loopt has implemented pattern monitoring to better identify non-legitimate users and potential misuse cases. These monitoring tools allow Loopt to enhance its privacy controls and customer-service response levels.

V. COOPERATION & POLICY OUTREACH.

Our accomplishments to date in terms of privacy and security innovation would not have been possible without the great work and insights of several key NGO partners. The expertise and know-how of these organizations makes ongoing collaboration with them a critical business practice for Loopt. Loopt is a member of the CTIA’s WIC Leadership Council, and actively participated in the creation of the “*CTIA LBS Best Practices*”. Loopt has also had discussions with dozens of congressional staff (Commerce, Judiciary

committees), FCC staff and commissioners, and FTC staff to help these individuals better understand our service and policies, and to solicit feedback.

Among other activities, Loopt's policy executives regularly participate in public forums to discuss these matters of online safety and privacy, including:

- Panelist; *Family Online Safety Institute's Annual Conference '07*
- Exhibitor; *State of Net '08, Advisory Committee to the Congressional Internet Caucus*
- Panelist; *2008 Cyber Safe California, California Office of Privacy Protection*
- Panelist; *Roundtable on Wireless Innovations, Tech Policy Summit '08,*
- Panelist; *Federal Trade Commission's Mobile Commerce Town Hall '08*
- Panelist; *The Focus on the Locus, Columbia University Institute for Tele-Information*
- Participant; *Kids, Media & Marketing Roundtable, Progress & Freedom Foundation*
- Panelist; *Online Safety Solutions Roundtable, Family Online Safety Institute*

In addition, Loopt is involved with leading mobile, social networking, and online privacy and security organizations such as the Family Online Safety Institute, Center for Democracy & Technology, Cyber Safe California, ConnectSafely.org, Congressional Internet Caucus Advisory Committee, Electronic Frontier Foundation, and the Progress & Freedom Foundation's Center for Digital Media Freedom. Loopt also works with the Community Concerns division of the California State PTA, which organization serves nearly one million local PTA members in California.

VI. LAW ENFORCEMENT COOPERATION.

Law enforcement cooperation is a critical part of Loopt's approach to online safety. Loopt has developed a thorough "Information Requests" policy, which has been made available on AskCALEA.net, and is otherwise available upon request. This policy describes for law enforcement the type of information available and the process by which law enforcement may lawfully request it. Loopt maintains a dedicated toll-free phone number and email address for law enforcement request purposes.

INTRODUCTION

Viacom/MTV Networks is one of the world's leading creators of entertainment content, with brands that engage and connect diverse audiences across television, online, mobile, games, virtual worlds and consumer products. Our portfolio spans more than 150 television channels and 350 digital media properties worldwide, from brands including MTV, VH1, Nickelodeon, Nick at Nite, COMEDY CENTRAL, CMT, Spike TV, TV Land and, Logo. Our digital sites are dedicated to building a social experience that is focused on media and connecting with friends around favorite shows, stars, artists and passions.

As we grow and enhance our digital media offerings, MTV Networks has made efforts to build a solid foundation in safety, security, and privacy on all of our websites. We have established standards and best practices in areas of content and contact that we continue to refine as the digital landscape continues to evolve.

SAFETY FEATURES

Enforcement of Minimum Age Requirements: All sites under MTV Networks Terms of Use have a minimum age restriction; currently set at 13 years old (please refer to “Special Considerations for our Child-Directed Websites” below). Sites targeting an older demographic are set at a higher minimum age. We have established policies to help enforce our minimum age restriction, including a drop down list that does not stop at the minimum age (implying the age required) and a neutral and difficult to circumvent rejection. MTVN also places a cookie on a registrant's browser to help prevent age falsification.

Email Verification: Our sites require that users register with a valid and/or authenticated email address in order to assist in verifying users and to discourage users from impersonating others.

Privacy Settings: Profiles of users that are under 16 are automatically set to private upon account creation and all users have the option to set their profiles to private. Users under 16 are prohibited from making their profiles public to users over 18 unless the user becomes “friends” with that user. Users 18 and over can only become “friends” with users under 16 if they know the user's last name, email address, or username. As an unregistered user or a user over 18, we do not allow searches for users under 18.

All interaction tools, private, instant and video messaging and user profiles have the “block user” function available and easily accessible. In addition, users can also choose to hide their ‘online now’ status and choose only to give their friends access to send messages for further privacy.

Automatic display of a user's last name is never allowed on any of our sites and usernames are automatically displayed instead.

We age- lock users into their selected age group 17 & under or 18 and over preventing them from bypassing important age based default safety features.

Pre-Moderation of Videos and Photos: Uploads are screened for copyright infringement and inappropriate content using human moderation and/or identification technologies. 24/7 human moderators are also on hand to resolve any potential issues/discrepancies with the automatic screening of videos (including avatars/profile pictures) for copyright infringement. Human moderators also screen uploads for any potential violation of our content moderation guidelines and terms of use. Although text is not pre-moderated each site has the ability to issue 'hot word replacements' for certain words to be auto-replaced by a string of selected characters. Word replacement applies to community pages and widgets and user profile pages, including module headers and display name.

Post Moderation & Reporting Tools: Our sites offer users the ability to report inappropriate content by flagging content and comments which are then reviewed by our moderators for further action if necessary. Also, available throughout the site is the ability to report a user, which is located directly on the user profile. Additionally, flags to report abuse are provided in other areas containing user-generated content, including photos, forum postings, and profile threads.

Rating Inappropriate Content: Our 24/7 moderation allows us to rate and filter (or an age gate when appropriate) content as suitable for either all ages, 13+,16+, 18+, or unacceptable.

Predatory Behavior Online: Built into our moderation practices is also a process for handling occurrences of child pornography and any signs of predatory behavior on our sites with a direct link to NCMEC's CYBERTIP line.

Education: We have implemented various age-appropriate educational tools for users across our sites such as internally produced safety pop-ups, video feeds and FAQ's. We include informative safety documents to assist both users and parents and include links to outside resources on safety, security and privacy (FTC) on our websites. We have also developed a comprehensive website for girls with vital safety information on how to protect themselves online.

Special Considerations for Our Child-Directed Websites: In addition to ensuring that the experience of our 13+ community is safe and secure, MTVN takes special precautions to safeguard the online experiences of our most vulnerable users, children under 13. All MTVN websites directed at children under 13 fully comply with the Federal Trade Commission's Children's Online Privacy Protection Act (COPPA). In addition, we do not collect PII at registration and children are always asked to register with a nickname.

Steps are also taken to ensure that children's safety is never at risk. In addition to all UGV and UGC being pre-moderated, all message board posts are also pre-moderated on children's sites. If chat functionality exists on one of the child-directed websites, the

functionality is accompanied by parental notifications and controls for each account. It is restricted to a list of prewritten phrases or a limited dictionary that has been vetted and includes a phrase filter that eliminates problematic word combinations.

CONCLUSION

Following our participation with the Berkman Internet Safety Task Force, we are exploring utilizing sex offender registry software to assist us in locating and removing RSO's from our sites. We are also evaluating filtering, auditing and text/contextual analysis systems. MTV Networks is committed to enhancing the safety, security and privacy on our sites. Moving forward, we will continue to research technical and non-technical solutions, while remaining involved with industry initiatives and self regulation efforts.



MySpace and its parent company, Fox Interactive Media, are committed to making the Internet a safer and more secure environment for people of all ages. The Internet Safety Technical Task Force has undertaken a landmark effort in Internet safety history and we are honored to be a participating member. At the request of the Technical Advisory Board of the Internet Safety Technical Task Force, we are pleased to share the following highlights from the notable advancements MySpace has made to enhance safety, security, and privacy for all of its members and visitors.

INTRODUCTION

MySpace.com (“MySpace”), a unit of Fox Interactive Media Inc. (“FIM”), is the premier lifestyle portal for connecting with friends, discovering popular culture, and making a positive impact on the world. By integrating web profiles, blogs, instant messaging, email, music streaming, music videos, photo galleries, classified listings, events, groups, college communities, and member forums, MySpace has created a connected community. As the first-ranked web domain in terms of page views, MySpace is the most widely used and highly regarded site of its kind and is committed to providing the highest quality member experience. MySpace will continue to innovate with new features that allow its members to express their creativity and share their lives, both online and off. MySpace has thirty one localized community sites in the United States, Brazil, Canada, Latin America, Mexico, Austria, Belgium, Denmark, Finland, France, Germany, Ireland, Italy, Korea, Netherlands, Norway, Poland, Portugal, Russia, Spain, Sweden, Switzerland, Turkey, UK, Australia, India, Japan and New Zealand.

MySpace’s global corporate headquarters are in the United States given its initial launch and growth in the U.S. MySpace has developed a close, cooperative working relationship with government policymakers, law enforcers, and NGOs, and we are committed to expanding our efforts to develop similar relationships in countries where we localize our site. Currently, we have been doing so in Australia, the United Kingdom, France, Italy, Brazil and other countries.

MySpace has exponentially evolved in an ever changing Internet world. When Fox Interactive Media and News Corp., acquired MySpace in 2005, the site had 22 million registered users. Today, this site has nearly 122 million monthly active users around the globe spanning 31 countries in 17 languages. The site currently handles approximately 20 million images and 105,000 videos uploaded per day.

MySpace has made efforts to build a foundation of safety, security, and privacy that encompasses technology development, user education, NGO partnerships, law

enforcement support, public policy initiatives, and industry cooperation. The work that MySpace does in this area strives to attain three goals which we often describe as the “Three C’s”:

- Content – prevent access to inappropriate content
- Contact – prevent unwanted contact
- Collaboration – partner with law enforcement, safety advocates, law makers, and educators to enhance safety, security, and privacy as a community and raise awareness in these areas

While the industry has historically taken a reactive approach, MySpace has endeavored to provide a combined reactive and proactive approach to safety, security, and privacy. As such, MySpace has implemented over 100 safety features and programs designed to increase user safety, security, and privacy in the past two years alone.

A central component of MySpace’s efforts is adopting, as closely as possible, safety features that society follows in the physical world into the online world. More specifically, MySpace takes a comprehensive and holistic approach that involves the following elements working together:

- Site-specific safety features, policies, and practices to address illegal and otherwise harmful content;
- Cooperation with law enforcement and collaboration to the extent permitted by law;
- Engaged and informed parents with access to tools to protect their children;
- Easy to use tools for members to protect themselves and their privacy and to report any abusive contact or content;
- Robust safety educational information available to members, parents, and teachers;
- Strong online safety legislation; and
- Collaboration with organizations that further promote online safety and education.

MySpace’s safety, security, and privacy program starts with a staff with a strong background in law enforcement and Internet safety issues. The worldwide program is headed by Hemanshu Nigam, a former U.S. Department of Justice Internet crimes prosecutor who also has held executive-level security positions at Microsoft and the Motion Picture Association of America. The MySpace global safety initiatives and law enforcement coordination are overseen by Jennifer Mardosz, also a former U.S. Department of Justice prosecutor who specialized in Internet crimes against children. MySpace has dedicated safety personnel based in Australia, the UK, France, Italy and Brazil. MySpace also works closely with John Carr, a renowned child protection advocate. Carr has a wide range of experience in this area, serving as Secretary of the UK’s Children’s Charities’ Coalition on Internet Safety, and as the former Head of the Children & Technology Unit at National Children’s Home as well as other positions in the field.

SAFETY FEATURES

MySpace has proactively sought to improve online safety by adopting and continuing to advance the safety features described below.

- ***Image and Video Review:*** MySpace reviews images and videos that are uploaded to the MySpace servers and photos deep-linked from third party sites for compliance with the Terms of Use and Photo/Video policy (which prohibit nudity, pornography, and sexually explicit images). If an image or video violates our Terms of Use, the content and possibly the entire profile are deleted. Hashing technology is also used to prevent inappropriate images from being uploaded a second time, after they have already been identified as inappropriate.
- ***Enforcing Age Limits:*** MySpace's Terms of Use have minimum age restrictions, currently set at 13 years old. While there is currently no effective age verification mechanism due to technical, legal, and data challenges, MySpace has adopted a number of technical solutions and procedures to enforce the age restriction. For example, the MySpace registration page requires prospective members to select their year of birth from a drop down menu currently ranging from 1908 to 2008, and individuals who enter a date that does not meet the requisite age are not permitted to register. MySpace also places a session cookie on the registration page so that a prospective member cannot change his/her age if the initial age was below that specified in our Terms of Use.

To combat a situation where an underage minor lies about his or her age, MySpace employs a strengthened search algorithm, utilizing terms commonly used by underage users, to find and delete underage profiles. The site is scanned for such terms, and the database of search terms is updated to reflect changes in user behavior and terminology.

Profiles that have been reported by MySpace members or parents as belonging to an underage user also are reviewed by MySpace. Whenever an underage user is identified, the profile is deleted. MySpace similarly will remove members if we believe they are over 18 and they represent themselves as under 18.

- ***Privacy Settings:*** All users have the option to set their profiles to private and profiles of users under 18 are automatically set to private upon account creation. The privacy setting for users under 16 prohibits any unsolicited contact or communication with users not given the status of friend who are over the age of 15. If users under 16 override their privacy settings, they are still only viewable by other users under 18. Users 18 and over can only become "friends" with users under 16 if they know the user's last name or email address.

Additionally, all users have the option to block users in specific age ranges from contacting them. Users under 18 can block users 18 and over from contacting

them or viewing their profiles and, alternatively, users 18 and over can block users under 18 from contacting them or viewing their profiles. All users also can conceal their 'online now' status, and can pre-approve all comments before allowing them to be posted to their profile or blogs.

Finally, upon registration minors are locked into their selected age preventing them from bypassing important age based safety features.

- ***Users Empowered to Report:*** MySpace offers users standardized methods to report inappropriate content to MySpace. Specifically, throughout the site there are links to "Contact MySpace" and a link to "Report Abuse" at the bottom of every MySpace user's profile. Additionally, links to report abuse are provided in other areas containing user-generated content, including emails, videos, photos and forum postings.
- ***Teachable Moments:*** For the safety and security of its users, MySpace blocks adult and malicious third party links and provides an interstitial warning page when following a link that takes a user outside MySpace.com. These instances provide the opportunity for teachable moments in which the user is taught about the reasons a link might be disabled or how to be cautious with their personal information outside of MySpace. Other teachable moments include safety tips that are required to be read in order for a minor to create an account, as well as warnings to exercise caution with personal information when updating your profile as a minor.
- ***Remove Registered Sex Offenders:*** MySpace is committed to adopting safety features from the physical world into the online setting. For example, convicted sex offenders are required to register their physical addresses on publicly available sex offender registries. MySpace partnered with Sentinel Tech Holding Corp. to build a database, called "Sentinel SAFE," which compiles all the registries into one centralized searchable database. We are currently comparing the Sentinel SAFE database against the MySpace database so we can remove registered sex offenders from our site. We are deleting the registered sex offenders' profiles and preserving the information for law enforcement.
- ***Crisis Intervention:*** The National Center for Missing and Exploited Children has developed a system to send emergency notifications to local communities via traditional communications (radio and television) when a child becomes missing. MySpace has partnered with NCMEC to distribute localized online AMBER Alerts on the MySpace site to help bring a missing child home as soon as possible. To date MySpace has served over 463,000,000 AMBER Alert impressions to its users.

MySpace has also partnered with safety and mental health organizations including the National Suicide Prevention Lifeline to help at risk teens connect with the experts who can assist them through a crisis.

- ***Email Verification:*** MySpace requires that users register with a valid and authenticated email address. This reduces spam, and helps law enforcement track down potential criminals by removing some of the anonymity of individuals by associating them with an actual email address.
- ***Resources for Parents:*** Parents worldwide can contact MySpace with any concerns they have about their teen’s account by selecting the “Contact MySpace” option at the bottom of every webpage. Messages submitted through the local “Contact MySpace” link are routed to a specialized team that will work with parents to resolve any issues, including deletion of a MySpace profile at a parent’s request. Parents are encouraged to alert us if there are areas of concern so that we can take appropriate action.

MySpace also introduced a ParentCare hotline and email (parentcare@myspace.com) for parents who need additional and personalized assistance resolving issues related to their teen’s use of MySpace. Through the ParentCare hotline and email, parents and guardians can contact MySpace via phone or email. Instructions for contacting ParentCare through the telephone hotline or via email can be found in the parents section of the MySpace Safety site, accessible from the Safety Tips link located at the bottom of every MySpace page or at <http://www.MySpace.com/safety>.

- ***Dedicated Team for Customer Care:*** Sensitive issues such as cyberbullying, impostor profiles, and harassment are handled by a special Customer Care team. This is a primary source of user problems, and our teams engage in labor intensive reviews of these issues to determine if the complaints are factual and then to determine the proper response.
- ***Parental Software:*** MySpace developed and released ParentCare, free software that, once downloaded onto a computer, identifies users who log into MySpace from that computer. The software reveals user-provided information (age, user name, and hometown) to parents so they will know whether their child has a MySpace profile and what age the child has claimed to be regardless of the computer that the child subsequently uses to log in to the site. The ParentCare software is designed to support MySpace’s special safety protections for community members under 18. By enabling parents to learn whether a teen has a MySpace profile and is using his or her accurate age, it helps to ensure those protections are in place to prevent unwanted adult contact with users under 18; stops underage users from joining MySpace; and prevents access to inappropriate content by users under 18.
- ***Preventing Teens from Accessing Age-Inappropriate Content:*** MySpace restricts the ability of younger users to access age-inappropriate content. For example, users under 18 are denied access to age-inappropriate areas such as

Romance & Relationship chat, forums, and groups; all groups designated as Mature; and Classified categories such as Personals and Casting Calls.

- **Crisis Communication:** MySpace in partnership with the Department of Homeland Security worked to distribute up to the minute severe weather information during the hurricane season. In the period following Hurricane Gustav, MySpace was the fourth largest referrer of traffic to DHS.gov.

MySpace is also working with universities to incorporate MySpace as one of the communication conduits in their emergency protocols to help keep students who are MySpace users informed during an emergency.

- **Group Review:** Using keyword tools, groups are proactively reviewed for inappropriate content. Inappropriate group content is removed with action taken against the group itself and the group's moderator if warranted.
- **Partnership with NCMEC:** Illegal content discovered by MySpace agents through proactive review is immediately reported to the National Center for Missing and Exploited Children. Additionally, MySpace empowers users to send a report directly to the Center by providing a direct link to the CyberTipline along with easy to follow instructions.
- **Closed School Section:** Users who wish to join a school forum for current students must be "vouched" for by existing student members. Requiring that the member be known to other students in the real world creates a natural barrier between current students and other users.

SECURITY FEATURES

FIM and MySpace recognize that users want a more secure experience online as well as a safer experience. MySpace has implemented many features to combat abuse of its service.

- **Interstitial Pages:** Interstitial pages appear when clicking on third party links. These pages inform users that they are leaving MySpace.com and to be mindful not to reveal their login information. Since the launch of these interstitial pages incidents of malicious fake login pages have dropped by 75%.
- **Comprehensive Spam Settings:** Users are empowered with over twenty communication preference options designed to allow them to restrict communication as strictly or as leniently as they choose. MySpace can guide users' settings if they choose to utilize one of three levels of preset options (low, medium, or high) or the user can customize their settings by enabling any individual options they wish.

- ***CAPTCHAs:*** CAPTCHAs are simple visual gateway puzzles designed to be solved easily by human users but difficult or impossible for computers to solve in an automated environment. By requiring CAPTCHA solutions to perform specific activities on MySpace, and by allowing users to have the option to require CAPTCHA solutions for certain methods of contact, MySpace has drastically reduced spam on its service.
- ***Phishlocking Tool:*** Spammers thrive on the inherent trust of communication users receive from friends to propagate their advertisements. MySpace has developed a tool which can detect user accounts that may have been phished and “lock” them, preventing the account from perpetuating the advertisement until the user can update their password and solve a CAPTCHA.
- ***MSPLINK Implementation:*** All third party links on MySpace are now converted into ‘MSPlinks’ which act as a wall between MySpace and outside websites. When a user posts a third party link on MySpace it is physically converted to a new link and routed through MSPlinks.com. In doing so, MySpace maintains control of third party links on its service and can “turn off” malicious or inappropriate links immediately and retroactively across the entire site. Even malicious links that are purposely malformed to deceive MySpace security tools can be recognized and disabled under this method.
- ***Pattern Tracking:*** MySpace utilizes a series of tools to identify anomalies in how a user might be using MySpace. These tools then allow MySpace to block and filter incoming connections to MySpace thus minimizing the presence of spammers and phishers on the site.
- ***Dedicated Team for Security Enforcement:*** A dedicated security team works to identify potential problems and takes immediate action when security issues occur.
- ***Users Empowered to Report:*** MySpace offers users consistent methods to report inappropriate content including spam and phishing pages. See section “Safety Features: Users Empowered to Report” for more information.
- ***Teachable Moments:*** See section “Safety Features: Teachable Moments” for more information.
- ***Application Security:*** Applications are widgets created by third party developers, often with interactivity that can be installed into users’ profiles and shared with other users. Prior to approval, all applications are reviewed by MySpace staff to ensure compliance with MySpace Developer’s Platform API’s and posted Application Guidelines such as those designed to prevent nudity and pornography.

See section “Privacy Features: Application Privacy” for more information.

- **Privacy Settings:** See section “Safety Features: Privacy Settings” for more information.

PRIVACY FEATURES

FIM and MySpace strive to enable users to determine the precise level of privacy they desire. In that vain, MySpace features customizable privacy features and options.

- **Email Notifications:** Users have the option to subscribe or abstain from seventeen types of email notification in relation to their account. Users can choose as much or as little contact from MySpace via email as they wish.
- **Privacy Settings:** Users have the ability to restrict access to specific posted content such as blogs, images, and videos. For instance a user can make an image visible to everyone, friends only, or only themselves. These settings allow MySpace users to choose from many levels of privacy.

See section “Safety Features: Privacy Settings” for additional information.

- **Friend Updates:** Users can not only control what updates they would like to receive from their selected friends, but also what updates are sent to their friends from their own profile regarding their activity on MySpace. Fourteen individual options allow a user to determine whether their friends are updated when they do anything from adding a new photo to posting a message in a forum. Once again, a user can choose as many or as few options as they wish.
- **Closed School Section:** See section “Safety Features: Closed School Section” for additional information.
- **Application Privacy:** Installation of these applications is entirely at the user’s discretion. MySpace users have the ability to block third party applications installed by others on their friends list from accessing their personal information. Users may also block all messages and comments from third party applications.

The measures outlined above are just a sample of the steps MySpace has taken to enhance user safety, security, and privacy. Please refer to the MySpace Safety and Security Overview at the end of this document for further information on some of the additional significant steps MySpace has taken to provide all of our users with a safer more secure online experience.

LAW ENFORCEMENT

MySpace has developed comprehensive Law Enforcement Guides for both U.S. and international law enforcement to explain how to obtain the information they may need from MySpace for their investigations. The Guides describe what type of information is available and the mechanisms by which law enforcement may lawfully request it. MySpace also maintains a 24/7 dedicated hotline and email address for use solely by law enforcement. To date MySpace has trained over four thousand law enforcement officers in addition to distributing over five thousand copies of the Law Enforcement Guide.

In partnership with sixteen law enforcement agencies across the U.S., MySpace has formed an Anti-Gang Task Force to explore the landscape of online gang activity. MySpace agents will take part in cross-training with detectives and officers from the Los Angeles Police Department's hardcore gang unit as a facet of this partnership.

Internationally, MySpace employs dedicated safety personnel located in three EU countries, UK, France, and Italy, as well as Brazil and Australia to serve as a liaison between local law enforcement and MySpace. Safety personnel help facilitate law enforcement inquiries by liaising with the US-based law enforcement team. They also implement safety programs and partnerships with local government agencies and NGOs.

LEGISLATIVE STRATEGY

MySpace believes that one of the best ways to fight crime on the Internet is to recognize that the web is every bit a neighborhood as our cities and towns and to modernize our laws with this reality. Our criminal laws from the offline world fit well in the online world, following the core principles of education, law enforcement support, and appropriate criminal penalties. In particular, MySpace works with government and legislators to promote legislation that is aimed at fighting sexual predator activity on the web.

- ***Email Registration for Sex Offenders:*** In the United States, most sex offender registries require registration only of physical addresses. MySpace is advocating that those sex offenders also be required to register their email addresses with the registries. That way, MySpace and other websites can then use that information to keep convicted sex offenders from signing up on their site. However, if a registered sex offender uses a false or unregistered email address, they would face criminal penalties. Twenty one states in the U.S. have passed such legislation and it has been introduced into numerous others. (Alaska, Arizona, Connecticut, Florida, Georgia, Hawaii, Illinois, Kansas, Kentucky, Louisiana, Maryland, Mississippi, Missouri, New York, New Hampshire, North Carolina, Oklahoma, Tennessee, Utah and Virginia.) In addition, the recently enacted KIDS Act has enacted a similar requirement for convicted sex offenders in the federal arena. Recently, the American Legislative Exchange Council adopted sex offender email registry legislation as part of a broad Internet safety "model bill," with the

likelihood of U.S. state adoption more broadly in 2009.

- ***Anti-grooming/Misrepresentation of Age to Solicit Minors Online:*** MySpace also supports legislation that makes it a crime for an adult Internet user to lie about his or her age with the intent to solicit a minor online for sexual purposes.
- ***Online Safety Education:*** We support legislation that mandates online safety education in our schools with the necessary funding to make it meaningful.
- ***Resources for Law Enforcement:*** We support legislation that increases funding and resources for law enforcement to investigate and prosecute crime in both the real and online worlds.

EDUCATION AND OUTREACH

MySpace firmly believes in the power of user education and collaborative outreach in the pursuit of improved online safety and has, therefore, worked with law enforcement, schools, community groups, and Internet users to educate its constituents. These are essential steps. As MySpace becomes increasingly popular, it will continue to pursue and foster these relationships with law enforcement agencies, education groups, NGOs and community representatives.

- ***Law Enforcement:*** MySpace provides training to cybercrime units in the U.S. and countries where it has safety personnel on how to investigate and prosecute cybercriminals using MySpace. MySpace also provides both a U.S. and international law enforcement guide to educate law enforcement officers worldwide about MySpace and provide contact information for a dedicated 24/7 hotline.
- ***Parents:*** Parents are an integral part of the effort to keep teens as safe as possible online. Therefore, we provide extensive educational resources for parents and teens on the site, including links to safety tips for parents and users that appear at the bottom of every page of the site. The Safety Tips section provides comprehensive guidelines on how to use MySpace safely. The parent Safety Tips are designed to educate parents about MySpace and how to help their teens make safe decisions in relation to their use of online communities. They also encourage parents to talk with their kids about how they communicate with others and how they represent themselves on MySpace.

Additionally, the Safety Tips provide parents with step-by-step instructions detailing how to remove their teen's profile from MySpace if they so desire, and links to free software that enables parents to monitor or block their teen's use of the Internet, including blocking MySpace. While every market can access the Safety Tips link at the bottom of every page, MySpace is in the process of editing

these Safety Tips for markets where we have localized sites to ensure locally relevant content.

MySpace also provides a link for parents to purchase books which provide safety tips for parents. “MySpace Unraveled,” written by renowned online safety experts Larry Magid and Anne Collier, reviews safety on MySpace specifically for parents. “MySpace, MyKids,” written by Internet safety expert Jason Illian, provides advice to parents on how to communicate with their children about online safety.

- **Teens:** MySpace spends significant resources educating teens on how to navigate the Internet safely and securely and about safety issues such as posting of personal information, cyberbullying, phishing and exposure to inappropriate material and contact. A great deal of progress has been made over the past few years in providing a variety of protections for teens using social networking sites like MySpace and the Internet in general. Research continues to show that teens are taking advantage of the tools and education they have been provided to protect themselves. However, more can be done to identify and provide support to those teens that are already at risk in the physical world, as those teens might also be at risk in the online environment despite the tools and education available to them.

Some relevant studies in this area include the following:

- Amanda Lenhart, *Teens, Stranger Contact & Cyberbullying*, Pew Internet & American Life Project (April 30, 2008), available at http://pewinternet.org/PPF/r/250/presentation_display.asp.
- Janis Wolak, et al., *Online “Predators” and Their Victims: Myths, Realities, and Implications for Prevention and Treatment*, American Psychologist, Vol. 63, No. 2 111-28 (Feb.-Mar. 2008), available at <http://www.apa.org/journals/releases/amp632111.pdf>. The authors state the social networking sites do not appear to have increased the risk of victimization by online molesters. *Id.* at 117.
- Michele L. Ybarra & Kimberly J. Mitchell, *How Risky Are Social Networking Sites? A Comparison of Places Online Where Youth Sexual Solicitation and Harassment Occurs*, Pediatrics (Jan. 28, 2008), available at <http://www.pediatrics.org/cgi/content/full/peds.2007-0693v1> (concluding that broad claims of victimization risk associated with social networking sites do not seem justified).
- Janis Wolak, et al., *1 in 7 Youth: The Statistics about Online Sexual Solicitations*, Crimes Against Children Research Center (Dec. 2007), available at <http://cyber.law.harvard.edu/sites/cyber.law.harvard.edu/files/1in7Youth.pdf>.
- Internet Caucus Advisory Committee, Panel Discussion, *Just the Facts About Online Youth Victimization: Researchers Present the Facts and*

Debunk Myths (May 2007), available at <http://www.netcaucus.org/events/2007/youth/20070503transcript.pdf>.

- Larry D. Rosen, *Adolescents in MySpace: Identity Formation, Friendship and Sexual Predators* (June 2006), available at <http://www.csudh.edu/psych/Adolescents%20in%20MySpace%20-%20Executive%20Summary.pdf>
- **Outreach to Educators:** MySpace has produced the “School Administrator’s Guide to Understanding MySpace and Social Networking Sites.” This guide addresses the specific needs and concerns that educators and school administrators may encounter on MySpace. The guide has been distributed to over 55,000 schools.
- **In Europe, MySpace has** been working with thirteen other multi-national technology and telecommunications companies as part of a newly formed industry partnership with a European education organization called European Schoolnet (EUN) to deliver a coordinated set of education and awareness materials aimed at teachers across Europe. See <http://en.teachtoday.eu/>
- **NGO Partnerships:** MySpace is also involved with, and dedicates resources to help, non-governmental organizations on Internet safety issues. Some U.S.-based safety organizations include IKeepSafe.org, NCMEC, Enough is Enough, Connect Safely and the Family Online Safety Institute. MySpace is developing a similar strategy for outreach in other countries.
- **Media Outreach:** MySpace has an extensive media reach and has used these abilities to increase public awareness about online safety, security, and privacy. MySpace has also launched Public Service Announcements (PSAs) on Internet safety, security, and privacy through News Corporation and Fox’s media platforms and other platforms targeted at both children and adults. This has included News Corporation and MySpace engagement in the largest PSA campaigns on Internet safety with NCMEC as well as the development of celebrity-based multimedia PSA campaigns on Internet safety via multiple media outlets, in addition to online PSAs. MySpace recently joined with Internet Keep Safe Coalition (www.ikeepSAFE.org) to release a broadcast PSA geared at encouraging parents to talk with their teens about their Internet use and help them make smart decisions online. The PSA aired across all Fox broadcast and cable networks, including during shows such as American Idol. This PSA reached an audience of over 150 million viewers. Also as part of this effort, FIM partnered with Common Sense Media and the PTA to launch a national television PSA campaign featuring “24” star Kiefer Sutherland. MySpace is exploring similar outreach activities for deployment outside of the U.S.

SETTING THE BAR FOR SOCIAL NETWORKING SAFETY

MySpace believes that social networking sites should engage in at least the following six safety practices as a minimum bar to entry into this area. We refer to these items as the “Big Six:”

- ***Review Images and Videos:*** Sites should find ways to review hosted images and videos, deleting inappropriate ones when found.
- ***Check Discussion Groups:*** Social networking sites should review discussion groups to find harmful subject matter, hate speech, and illegal behavior, deleting that content when it is found.
- ***Remove Registered Sex Offenders:*** Social networking sites should ban registered sex offenders from setting up accounts on their sites using technology that already exists today.
- ***Enforce Minimum Age Requirements:*** Sites should enforce their minimum age requirements and take steps to identify and remove underage users who have misrepresented their age to gain access.
- ***Protect Younger Users from Adults They Don’t Know:*** Social networking sites should implement default privacy settings that prevent adults from contacting teens under 16 who they do not already know in the physical world.
- ***Partner with Law Enforcement and Other Experts:*** All sites should have law enforcement hotlines available at all times to assist law enforcement during emergencies and on routine inquiries. In addition, sites should engage experts in pertinent fields to enhance site safety.

CONCLUSION

MySpace is committed to a continued public private partnership to enhance safety, security and privacy. In connection with this commitment, we are working with law enforcement, governments, and NGOs in the myriad of ways described above, including promoting the adoption of site-specific safety measures, a targeted legislative strategy, and collaborative efforts.

APPENDICES

The above information represents much of the effort that MySpace has made on behalf of its users’ safety, security, and privacy. In addition, please find the following information:

Appendix A: A comprehensive overview of MySpace safety, security, and privacy features.

Appendix B: Joint Statement on Key Principles of Social Networking Sites Safety

APPENDIX A



MySpace Safety, Security and Privacy Overview

MySpace is committed to making our community as safe as possible for all of our members. Safety, security, and privacy are built into every new site feature and we have designed and built features specifically to enhance the security of our online community. This is an ongoing process that we are constantly reviewing and updating under the leadership of our Chief Security Officer, Hemanshu Nigam, who spent 18 years as a career prosecutor and child safety advocate. Nigam is a former Department of Justice Internet crimes prosecutor who held executive-level security positions at Microsoft and the MPAA and who leads a team that works full-time on safety and security-related initiatives across the company. In addition, MySpace has a robust team dedicated to policy enforcement and content review that work to identify potential problems and takes immediate action when safety and/or security issues occur.

We work hard to provide users with access to age appropriate content, to shield younger users from older members of the community, and to partner with law enforcement in these efforts. Some of the most significant steps we have taken in this area include:

Preventing Underage Users

- Our Terms of Use indicate that users must be 13 yrs of age or older to utilize our site
- We employ a search algorithm, utilizing terms commonly used by underage users, to seek and weed out individuals misrepresenting their age
- Additionally, our team actively searches out underage users by hand
- We delete thousands of profiles per week for misrepresenting their age

Protecting Younger Users from Inappropriate Contact

- Users under 18 are automatically assigned a Private Profile upon account creation
- No user can browse for users under 16
- Adults can never add under 16's as a friend unless they know the under 16's last name or email address (adult must know the user in the physical world)
- If users under 16 override their privacy settings, they are still only viewable by other users under 18
- Mature groups cannot be accessed by under 18's

- Users under 18 can block all users over 18 from contacting them or viewing their profile
- 13-15 yr olds are tagged to be un-searchable by age on search engines
- 13-15 yr olds can only receive group invites from the individuals in the friend network
- Users under 18 cannot access age-inappropriate areas such as Romance and Relationship chat, forums and groups, Mature groups and certain Classified categories including dating and casting calls
- Users under 18 cannot browse for age inappropriate categories such as relationship status, smoker, drinker, or income
- Users over 18 are limited in their ability to search in the School section- they can only search for high school students graduating in the current or upcoming year
- The creation and implementation of an adult website database that restricts users from posting mature links on their profile

Protecting Younger Users from Inappropriate Content

- Hosted images and videos are reviewed for compliance with Terms of Use (this includes over 10 million new images and videos uploaded everyday)
- Known inappropriate URLs are blocked from being posted on the site
- IP logs of image uploads are captured
- User accounts deleted for uploading pornographic videos
- Alcohol related ads prohibited from reaching under 21's
- Smoking/Drinking preferences blocked for under 18's/under 21's
- Groups and classifieds are reviewed when inappropriate content is suspected
- Users under 18 are defaulted in a way that requires them to pre-approve all comments made on their profiles

Reporting Inappropriate Content

- Users can report inappropriate content or behavior to MySpace
- Users can report spam email complaints to MySpace
- Users can directly report sexually explicit conduct to NCMEC's CyberTipLine
- Users can easily "Report Abuse" in email, videos, forum posts and classifieds
- Users are easily able to provide reasons when reporting images for Terms of Use violations

Providing Tools for all Members

- All users can set profile to Private
- Users can pre-approve all comments before being posted
- Users can block another user from contacting them
- Users can conceal their 'online now' status
- Users can prevent forwarding of their images to other sites
- Users over 18 can block users under 18 from contacting them or viewing their profile
- All users can allow only those users whom they have proactively added to their Contact List to see when they are on IM and to contact them

- Users can make all their photos, or sections of their photos, Private
- 32,000 school moderators oversee school forums

Providing Education

- All users under 18 receive security warnings before posting content
- All users under 18 must review and scroll through Safety Tips when they sign-on to the site
- Safety Tips link on every page which includes links to parent monitoring and blocking software
- Contact MySpace link on every page
- MySpace Parent Brochure available on Parent Safety Tips page
- School Administrator's Guide to Understanding MySpace and Social Networking Sites distributed to over 55,000 schools.
- Aggressive education campaign through MySpace, News Corp properties, and third-party partners including National Center for Missing & Exploited Children, National PTA, AdCouncil, Seventeen Magazine, National School Board Association & the National Association of Independent Schools.
- Extensive PSA campaigns across News Corp properties

Partnering with Non-profit Organizations

- Partnerships with the Illinois Library Association and the American Library Association to distribute millions of bookmarks on Internet safety in public libraries across the U.S.
- AMBER Alerts: MySpace partners with the National Center for Missing & Exploited Children to distribute localized online AMBER alerts via MySpace so MySpace users can help bring a missing child home
- Education Partnerships with organizations such as ConnectSafely.com, NetFamilyNews.com, WiredSafety.org, I Keep Safe Coalition (iKeepSafe.org), Cyberbullying 411, Enough is Enough and MySpace MyKids
- The donation of Sentential SAFE to NCMEC
- Participate in the UK Government Taskforce on Child Safety on the Internet
- Contributed to the UK Home Office Taskforce's first UK Social Networking Guidance
- Participate in the UK Government's Cyberbullying TaskForce
- Participate in the Australian Government's Consultative Working Group on Cyber-Safety
- Participate in the EU Social Networking Task Force

Partnering with Law Enforcement

- Ongoing support for local, state, and federal law enforcement in investigations and prosecutions
- 24/7 dedicated hotline and email created for use by law enforcement – not just for emergencies
- Ongoing training provided to cyber crime units on how to investigate and prosecute cyber criminals using MySpace

- Law Enforcement Guide and One Sheet created to help law enforcement agencies understand MySpace and investigate cases

Dedicated MySpace Teams

- Customer Care Team: handles sensitive user issues within 72 hours
- Content Assurance Team: ensures integrity of safety systems and flags potential flaws
- Parent Care Team: dedicated parent hotline, email (parentcare@myspace.com) and guidebook
- School Care Team: dedicated educator hotline, email (schoolcare@myspace.com) and guidebook
- Law Enforcement Team: dedicated hotline, email (lawenforcement@myspace.com) and guidebook
- Security Incident Response Team: dedicated security team that works to identify potential problems and takes immediate action when security issues occur

Application Information and Data Collection

- Applications are governed by the same privacy controls that are in place for members
- An application can only get information from the user if the user installs the application and thereby grants the application permission
- MySpace offers a universal setting for not sharing any data, including public information, with any applications

Application Security

- All applications must use our API's, which have security features built in
- All applications go through a robust security review process before going live to our members
- MySpace takes action against applications that violate safety and security requirements

Taking Ongoing Safety/Security Measures to Spot & Solve Safety Challenges

- Email verification required for all new MySpace members
- ParentCare: MySpace developed software, called ParentCare, to help parents easily determine whether their teen has a MySpace profile, learn about safety and to ensure their teen's age is accurate.
- Email Registration Legislation: MySpace supports and has testified in favor of, federal and state legislation that would require registered sex offenders to register all of their email addresses, so that we can block them from accessing our site in the first place.
- Joint Statement on Key Principles of Social Networking Safety: MySpace and Attorneys General in the Multi-State Working Group on Social Networking representing 49 states and the District of Columbia joined forces to unveil a Joint Statement on Key Principles of Social Networking Safety designed for industry-

wide adoption. This common set of Principles relates to online safety tools, technology, education and law enforcement cooperation.

These measures represent just a sampling of the steps MySpace has taken to protect our community's safety and enforce our rules.

APPENDIX B



JOINT STATEMENT ON KEY PRINCIPLES OF SOCIAL NETWORKING SITES SAFETY

MySpace and the Attorneys General have discussed social networking sites safety measures with great vigor over several months. MySpace and the Attorneys General agree that social networking sites are a powerful communications tool that provides people with great social benefits. However, like all communication tools, social networking sites can be misused as a means to commit crimes against minors and can allow minors to gain access to content that may be inappropriate for them.

MySpace and the Attorneys General recognize that millions of minors across the world access the Internet each day, and that many of these minors create social networking profiles on MySpace and other social networking sites. Based on recommendations MySpace received from the Attorneys General and online safety advocates, and as a result of its internal safety and engineering teams, MySpace has implemented technologies and procedures to help prevent children under 14 from using MySpace and to help protect minors age 14 and above from exposure to inappropriate content and unwanted contact by adults. The Attorneys General commend MySpace for its efforts to address these issues. They also call upon other social networking services to adopt these principles.

MySpace and the Attorneys General agree that additional ways to protect children should be developed. This effort is important as a policy matter and as a business matter.

PRINCIPLE: Providing children with a safer social networking experience is a primary objective for operators of social networking sites.

I. ONLINE SAFETY TOOLS

PRINCIPLE: Technology and other tools that empower parents, educators and children are a necessary element of a safer online experience for children.

PRINCIPLE: Online safety tools, including online identity authentication technologies, are important and must be robust and effective in creating a safer online experience, and must meet the particular needs of individual Web sites.

- MySpace will organize, with support of the Attorneys General, an industry-wide Internet Safety Technical Task Force (“Task Force”) devoted to finding and developing such online safety tools with a focus on finding and developing online identity authentication tools. This Task Force will include Internet businesses, identity authentication experts, non-profit organizations, and technology companies.

FORMED and ONGOING, LED BY HARVARD LAW SCHOOL’S BERKMAN CENTER FOR INTERNET & SOCIETY

- The Task Force will establish specific and objective criteria that will be utilized to evaluate existing and new technology safety solutions.
- MySpace and other members of the Task Force will provide adequate resources to ensure that all reasonable efforts are made to explore and develop identity authentication technologies.

DONE

- News Corporation will designate a senior executive to work with the Task Force.

DONE

- The Task Force will provide the Executive Committee of the Attorneys General Social Networking Working Group (“Executive Committee”) with quarterly reports of its efforts and presentation of a formal report by the end of 2008. The Executive Committee will have continuing access to the Task Force and the designated senior executive of News Corporation.

ONGOING

II. DESIGN AND FUNCTIONALITY CHANGES

PRINCIPLE: Development of effective Web site design and functionality improvements to protect children from inappropriate adult contacts and content must be an ongoing effort.

- MySpace and the Attorneys General share the goal of designing and implementing technologies and features that will make MySpace safer for its users, particularly minors. More specifically, their shared goals include designing and implementing technologies and features that will (1) prevent underage users from accessing the site; (2) protect minors from inappropriate contact; (3) protect minors from inappropriate content; and (4) provide safety tools for all MySpace users.

- The Attorneys General acknowledge that MySpace is seeking to address these goals by (1) implementing the design and functionality initiatives described in Appendix A; and (2) working to implement the design and functionality initiatives described in Appendix B.
- MySpace and the Attorneys General will meet on a regular basis to discuss in good faith design and functionality improvements relevant to protecting minors using the Web site.

ONGOING (2 written reports submitted regarding the status of implementation of new initiatives, and 1 conference call with Executive Committee members regarding the status of implementation of new initiatives)

III. EDUCATION AND TOOLS FOR PARENTS, EDUCATORS, AND CHILDREN

PRINCIPLE: Educating parents, educators and children about safe and responsible social networking site use is also a necessary part of a safe Internet experience for children.

- MySpace will continue to dedicate meaningful resources to convey information to help parents and educators protect children and help younger users enjoy a safer experience on MySpace. These efforts will include MySpace’s plan to engage in public service announcements, develop free parental monitoring software, and explore the establishment of a children’s email registry.

<i>PSA:</i>	<i>DONE</i>
<i>MySpace and iKeepSafe Tutorials:</i>	<i>DONE</i>
<i>Parent Care Software:</i>	<i>DONE</i>
<i>Parent Care Hotline:</i>	<i>DONE</i>
<i>Parent Care Email:</i>	<i>DONE</i>
<i>Parent Guide:</i>	<i>DONE</i>
<i>New MySpace Safety Tips:</i>	<i>DONE</i>

- MySpace shall use its best efforts to acknowledge consumer reports or complaints received via its abuse reporting mechanisms within 24 hours of receiving such report or complaint. Within 72 hours of receiving a complaint or report from a consumer regarding inappropriate content or activity on the site, MySpace will report to the consumer the steps it has taken to address the complaint.

Reports or complaints received through Report Abuse acknowledged within 24 hours – DONE.

Design modifications to extend ability to acknowledge within 24 hours reports/complaints submitted through other mechanisms, and to report back to the consumer on steps taken within 72 hours, have been developed and approved internally. Awaiting review by Independent Examiner before implementation.

- For a two (2) year period MySpace shall retain an Independent Examiner, at MySpace's expense, who shall be approved by the Executive Committee. The Independent Examiner shall evaluate and examine MySpace's handling of these consumer complaints and shall prepare bi-annual reports to the Executive Committee concerning MySpace's consumer complaint handling and response procedures, as provided above.

DONE

IV. LAW ENFORCEMENT COOPERATION

PRINCIPLE: Social networking site operators and law enforcement officials must work together to deter and prosecute criminals misusing the Internet.

- MySpace and the Attorneys General will work together to support initiatives that will enhance the ability of law enforcement officials to investigate and prosecute Internet crimes.
- MySpace and the Attorneys General will continue to work together to make sure that law enforcement officials can act quickly to investigate and prosecute criminal conduct identified on MySpace.
- MySpace has established a 24-hour hot line to respond to law enforcement inquiries. In addition, News Corporation will assign a liaison to address complaints about MySpace received from the Attorneys General. MySpace will provide a report on the status of its response to any such complaint within 72 hours of receipt by the liaison.

DONE

LAW ENFORCEMENT GUIDES ISSUES TO OVER 5000 LAW ENFORCEMENT OFFICERS.

TRAINED OVER 4000 LAW ENFORCEMENT OFFICERS IN PERSON.

APPENDIX A: DESIGN AND FUNCTIONALITY CHANGES

Preventing Underage Users

1. Browse function - limit to 68 years and below.

DONE

2. MySpace will implement “age locking” for existing profiles such that members will be allowed to change their ages only once above or below the 18 year old threshold. Once changed across this threshold, under 18 members will be locked into the age they provided while 18 and older members will be able to make changes to their age as long as they remain above the 18 threshold. MySpace will implement “age locking” for new profiles such that under 18 members will be locked into the age they provide a sign-up while 18 and older members will be able to make changes to their age as long as they remain above the 18 threshold.

DONE

Protecting Younger Users from Inappropriate Contact

1. Users able to restrict friend requests to only those who know their email address or last name.

DONE

2. “Friend only” group invite mandatory for 14 and 15 year olds.

DONE

3. “Friend only” group invite by default for 16 and 17 years olds.

DONE

4. Users under 18 can block all users over 18 from contacting them or viewing their profile.

DONE

5. Users over 18 will be limited to search in the school section only for high school students graduating in the current or upcoming year.

DONE

6. Users over 18 may designate their profiles as private to users under 18, and users under 18 may designate their profiles as private to users over 18.

DONE

7. Limit search engine ability to crawl all private profiles.

DONE

8. Users under 18 cannot designate themselves as swingers.

DONE

9. Users under 16 are automatically assigned a private profile.

DONE

10. Users over 18 cannot browse for users under 18.

DONE

11. A user cannot browse for users under 16.

DONE

12. Users over 18 cannot add users under 16 as friends unless they know the under 16 user's last name or email address.

DONE

13. Personally identifiable information removed upon discovery.

DONE

14. Users under 18 cannot browse for swingers.

DONE

15. MySpace will not allow unregistered visitors to the site to view any search results related to mature areas of the site, profiles that are private to under 18s, or other groups and forums geared toward sexual activity and mature content.

DONE

16. MySpace will change the default for under 18 members to require approval for all profile comments.

DONE

17. MySpace will remove the ability for under 18 members to browse the following categories: relationship status, “here for”, body type, height, smoke, drink, orientation and income.

DONE

18. If users under 16 override their privacy settings, they are still only viewable by other users under 18.

DONE

19. When user posts images, they will receive a note including IP address of the computer that uploaded the image.

DONE

20. Add sender URL in mail for private messages.

DONE

21. Locate underage users (searching specific keywords, reviewing groups and forums, and browsing certain age ranges).

DONE

22. Profiles of Registered Sex Offenders identified through Sentinel SAFE technology are reviewed and, once confirmed, are removed from the site. The associated data are preserved for law enforcement.

DONE

Protecting Younger Users from Inappropriate Content

1. Implementation of image policy for hosted images that employs hashing technology to prevent inappropriate image uploads.

DONE

2. Expand flag spam/abuse to allow categorization of flagged message.

DONE

3. Expand “Report Image” functionality to include a drop down menu that provides members with greater specificity on why they are reporting image. Categories to include Pornography, Cyberbullying, and Unauthorized Use.

DONE

4. Under 18s/under 21s cannot access tobacco/alcohol advertisements.

DONE

5. MySpace and Attorneys General commit to discuss with Google the need to cease directing age inappropriate linked advertisements to minors.

DONE

6. Events may be designated for all ages, for 18 + or for 21+.

DONE

7. MySpace will notify users whose profiles are deleted for Terms of Service Violations.

DONE

8. Groups reviewed for incest, hate speech or youth sex subjects with violators removed from site.

DONE

9. Members determined to be under 18 to be removed from mature Groups.

DONE

10. Posts determined to be made to mature Groups by under 18 members to be removed.

DONE

11. Any mature Groups determined to be created by under 18 members will be removed entirely and the user accounts may be deleted for violating the Terms of Service.

DONE

12. Users under 18 to be denied access to Romance & Relationships Forum and Groups.

DONE

13. Users under 18 will not have access to inappropriate parts of Classifieds (dating, casting calls).

DONE

14. Members may request to label Groups they create as mature.

DONE

15. Flagged Groups are reviewed and categorized by MySpace staff.

DONE

16. Members under 18 and non-registered users may not enter or view a Group page that has been designated as mature.

DONE

17. MySpace hired a Safety Product Manager.

DONE

18. Smoking/Drinking preferences blocked for under 18s/under 21s.

DONE

19. User accounts promptly deleted for uploading child pornographic images and/or videos and referred to NCMEC.

DONE

20. MySpace does not tolerate pornography on its site, and users determined to have uploaded pornographic images and/or videos flagrantly and/or repeatedly will have their accounts deleted.

DONE

Providing Safety Tools Protective Tools For All Members

1. All users may set profile to private.

DONE

2. All users can pre-approve all comments before being posted.
DONE
3. Users can block another user from contacting them.
DONE
4. Users can conceal their “online now” status.
DONE
5. Users can prevent forwarding of their images to other sites.
DONE
6. MySpace adds “Report Abuse” button to Email, Video, and Forums.
DONE
7. Users over 18 can block under 18 users from contacting them or viewing their profiles.
DONE
8. All users can allow only those users whom they have proactively added to their Contact List to see when they are on IM and to contact them.
DONE
9. “Safety Tips” Available on every page of MySpace.
DONE
10. “Safety Tips” Appear on registration page for anyone under 18.
DONE
11. Users under 18 must affirmatively consent that user has reviewed the Safety Tips prior to registration. MySpace will require under 18 members to scroll through the complete Safety Tips upon registration. MySpace will also require under 18 members to review the Safety Tips on an annual basis.
DONE

12. Additional warning posted to users under 18 regarding disclosure of personal information upon registration.

DONE

13. Safety Tips are posted in the “mail” area of all existing users under 18.

DONE

14. Safety Tips contain resources for Internet Safety including FTC Tips.

DONE

15. Phishing warning added to Safety Tips.

DONE

16. Safety Tips for Parents provides links to free blocking software.

DONE

17. Parent able to remove child's profile through the ParentCare Hotline and ParentCare Email.

DONE

18. MySpace will have “Tom” become a messenger to deliver Safety Tips to minors on MySpace.

DONE

19. All users under 18 receive security warnings before posting content.

DONE

APPENDIX B: DESIGN AND FUNCTIONALITY INITIATIVES

MySpace will continue to research and develop online safety tools. Based on recommendations MySpace received from the Attorneys General and online safety advocates, and as a result of the work of its internal safety and engineering teams, MySpace’s current plans include the following initiatives:

Limiting MySpace Membership to Users 14 and Over

1. Engage a third-party to build and host a registry of email addresses for children under 18. Parents would register their children if they did not want them to have

access to MySpace or any other social networking site that uses the registry. A child whose information matches the registry would not be able to register for MySpace membership.

Ongoing: MySpace heard presentations from Aristotle, GB Group, Privo and Sentinel regarding an email registry. Sentinel presented registry technologies at the June 20th Task Force meeting and heard significant criticism, leading them to withdraw their proposal. Policy and privacy challenges may prevent implementation of the registry.

2. Strengthen the algorithm that identifies underage users.

New algorithm has been created and is being tested. The solution implemented here is going to be basis for improvements in the Groups area of the site.

Protecting Minors from Unwanted Contacts by Adults

1. Change the default setting for 16-17 year olds' profiles from "public" to "private."

DONE for new users; will implement for existing users

2. Create a closed high school section for users under 18. The "private" profile of a 16/17 year old will be viewable only by his/her "friends" and other students from that high school who have been vouched for by another such student. Students attending the same high school will be able to "Browse" for each other.

Engineering ongoing

Protecting Minors from Exposure to Inappropriate Content

1. MySpace will review models for a common abuse reporting icon (including the New Jersey Attorney General's "Report Abuse" icon). If MySpace determines that a common icon is workable and will improve user safety, it may substitute the common icon for the current report abuse icon MySpace places on each member profile.

In discussions with General Milgram's office and others while reviewing Report Abuse models to see if any are superior to the standardized MySpace Report Abuse link.

2. Obtain a list of adult (pornographic) Web sites on an ongoing basis and sever all links to those sites from MySpace.

DONE; updated bi-monthly.

3. Demand that adult entertainment industry performers set their profiles to block access to all under 18 users.

DONE

4. Remove all under 18 users from profiles of identified adult entertainment industry performers.

DONE; system in place, ongoing process.

5. Retain image review vendor(s) that can effectively and efficiently identify inappropriate content so it can be removed from the site more expeditiously.

DONE

6. Investigate the use of an additional image review vendor to provide automated analysis of images to help prioritize images for human review.

Ongoing: Reviewed new vendors and retained independent consultant to continue vendor review.

7. MySpace will (1) develop and/or use existing technology such as textual searching; and (2) provide increased staffing, if appropriate, in order to more efficiently and effectively review and categorize content in “Groups.” MySpace will update the Attorneys General concerning its efforts to develop and/or use textual searching on a quarterly basis. Upon implementation of textual searching, the Attorneys General will review its efficacy with respect to “Groups”.

Ongoing; See comments under Algorithm section.

=/END/=



Internet Safety Task Force Request for Information

1. What safety issues do you attempt to address on your site? How do you measure the risk that youth face on your site?

With the multitude of global products and services within the Yahoo! network we, take a multi-faceted approach to child safety. Not only do we address network-wide issues such as the need for general child safety education, but we focus on the challenges specific to certain products. These challenges include distribution of child pornography, cyberbullying or other inappropriate or abusive conduct, and limiting minors' access to adult content. Yahoo! also works to provide tools that empower users to customize their experiences and help create a safer experience for their families. These customization tools also address safety challenges by allowing users to take action to prevent unwanted contact or exposure to unwanted content. Similarly, we tailor our education materials, safety guidance, and abuse reporting based on the service(s) and tools offered on each product.

While Yahoo! is not in the best position to track trends and collect data related to online safety issues, we work in partnership with educators, industry peers, law enforcement, and other child safety experts to guide our efforts, to collaborate with us on how best to address child safety issues on our network, and to benefit from their expertise in implementing safety features and programs. Specifically, we work closely with NCMEC's NetSmartz, iSafe, iKeepSafe, Wired Safety, Connect Safety, and Commonsense Media. We consult these groups and individual safety experts regularly on an individual basis and also collectively through informal conversations, sharing of program ideas, and formal training events for Yahoo! employees.

We also engage in outreach in our communities. For example, we recently held our second annual CyberCitizenship Summit at our Sunnyvale Campus. The Summit brought together Educational leaders from across California and safety experts from across the United States to discuss the challenges students and schools are facing online. Events such as the Summit provide valuable input for Yahoo! on how best to use our resources to address the most pressing safety concerns for kids and teens. In addition, through our regular training and interactions with law enforcement, we are able to learn about the trends law enforcement sees and their areas of concern. We have consulted with child exploitation experts in the law enforcement community to identify specific safety challenges to better enable Yahoo! to develop a response.

2. What technical (and non-technical) efforts have you undertaken to make your site safer for youth? Please list all features, policies, collaborations, etc. Indicate which safety issues these efforts attempt to address and which age groups are targeted in this approach. Please note if these are in-house efforts or if they are outsourced or a part of a collaboration and, if so, who your partners are. For each effort, please indicate your metrics for success.

Yahoo has been an industry leader in making our services safer for youth, through technical and non-technical means. The technical measures Yahoo! has developed in-house include:

- **Report Abuse Links:** Yahoo! provides tools to assist in reporting inappropriate or harmful behavior such as our “Report Abuse” links. Our report abuse feature is meant to help us address several issues, including distribution of offensive or illegal content, online harassment or cyberbullying, and misuse of email or instant messaging services. Report abuse functionality is included on various sites across the Yahoo! network, including Yahoo! Messenger, Flickr (photo-sharing site), Profiles, Yahoo! Answers, and Yahoo! Personals. Report Abuse buttons are focused on empowering all Yahoo! users, regardless of age.
- **SafeSearch:** Yahoo! provides the option of a “SafeSearch” feature to prevent display of adult content in search queries. The feature is designed to help shield users under age 18 from unwanted exposure to adult content. Parents can lock SafeSearch on to prevent children from turning it off. On Yahoo!’s mobile search service “oneSearch,” all users default to SafeSearch mode and children registered as under 18 cannot turn the function off.
- **Kid Search:** Yahoo! Kids features search results that have been human-reviewed by trained editors for age appropriateness and safety for children. In addition, Kid Search aims to prevent the display of adult content in search results responsive to search queries made on the Yahoo! Kids site.
- **Privacy features:** We build safety and privacy features into our products, including privacy preferences and blocking capabilities. These features give users the ability to control who can contact them using services such as Yahoo! Messenger, Answers, and Profiles. Users can block other users for any reason, but the functionality is chiefly designed to address the problems of online harassment, cyberbullying, spam, delivery of objectionable content, and grooming of children by predators.
- **Detection of inappropriate and illegal material:** Yahoo! has implemented technology and policies to help us identify apparent child pornography violations on our network. These include filters, algorithms, and human review, as well as user reports of abuse. These processes work in the background and are designed to protect users of all ages from potentially viewing illegal content.
- **Family Accounts:** Yahoo! provides a parent or legal guardian the option of opening a Yahoo! sub-account for their child under the age of 13 by charging a one time 50-cent fee to their credit card to ensure that a parent or legal guardian is involved in the account creation. Yahoo! donates a portion of the fee to help NCMEC’s efforts to protect children.

In addition to these in-house technical measures, Yahoo! also works with its partners to provide Parental Controls. Yahoo! makes available a Parental Controls product to Yahoo! users who have broadband Internet access through Verizon or AT&T. Our parental controls empower parents to limit the sites to which their kids can visit, thereby limiting children’s exposure to what the parent deems inappropriate content.

Yahoo also has undertaken several non-technical efforts to protect our users online. Our Yahoo! Kids site was an industry leader when it launched in 1996, and it continues to be a unique ‘green

space' in the industry today. Meanwhile, our Yahoo! Safely site provides kids, teen, and parents with a wide variety of safety content, including blogs, tutorials, videos and games.

In addition to our product-specific "Help" sections, tutorials, and safety and responsible usage tips for our users, we have partnered with domestic and international children's safety organizations, law enforcement, and others in the industry to address online safety concerns.

For example, Yahoo! has partnered with the National Center for Missing and Exploited Children (NCMEC) and the U.K.-based Internet Watch Foundation (IWF) in an effort to reduce the proliferation of child pornography by removing URLs hosting known images of apparent child pornography from Yahoo! search index results and responding to detection of these URLs or other images of apparent child pornography on our network.

Yahoo also partners with public safety officials to improve the safety of our sites and services. Yahoo! has created a 24 x 7 dedicated compliance team that can immediately respond to law enforcement if we are contacted about a situation that indicates that a child may be in danger. In addition, Yahoo! 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 part of this training and outreach effort, we have created a Law Enforcement Compliance Manual to educate law enforcement personnel about Yahoo!'s policies, procedures, and systems, and to help law enforcement better understand how to obtain the appropriate investigatory information in child exploitation cases.

Another aspect of our comprehensive approach to online safety includes collaboration with our industry partners. Yahoo! participates in the Financial Coalition Against Child Pornography, which brings together financial institutions such as banks, payment companies, credit card issuers, internet service providers, and NCMEC in an effort to eliminate commercial child pornography by taking action on the payment systems used fund such illegal operations. Yahoo! also has joined with NCMEC and internet service providers, including AOL, Google, Microsoft, Earthlink, and United Online, to create the industry Coalition for Child Protection Technology. The Coalition is dedicated to developing shared technologies aimed at fighting child pornography. Furthermore, through our work with NCMEC, we allow users to receive state or local Amber Alerts through their email, instant messaging and mobile services.

In addition, Yahoo! participates in a number of industry working groups organized by our non-profit partners Internet Keep Safe Coalition, FOSI.org, and the Ad Council.

Finally, Yahoo! donates millions of dollars worth of Public Service Announcements on child safety issues through banner ads across our network and sponsored links to sites our non-profit partner sites such as NCMEC's Netsmartz.org for elementary school age kids and their parents.

3. What results can you share about the actual impact of your various efforts in #2 to date? Please be as specific and data-driven as possible. What lessons have you learned from your efforts to execute in #2? If any of your approaches have not been as successful as you hoped or have had unexpected consequences, please provide a detailed case study.

Our product efforts are based on the guidance and input we receive from our various partners, as noted above, based on their research and expertise in this area.

It is extremely difficult to measure the impact of our efforts through specific data and statistics. For example, a decrease in the number of complaints we receive regarding the instances of offensive materials accessed by children could be due to an increased use of parental controls or

safe search or greater parental involvement (*i.e.*, education). At a hypothetical level, how would it be possible to quantify the number of unwanted adult-child contacts that never happened and then attribute those non-events to a particular technology?

There have been recent studies suggesting that online safety education efforts are bearing fruit, however. A recent study from the University of New Hampshire found that minors are receiving fewer unwanted online sexual solicitations online – only 1 in 7 in 2005 compared to 1 in 5 in 1999-2000. The study's authors attribute this success to education and media efforts which discourage children from visiting chat rooms or interacting with people they don't know.

4. What can you share about any efforts you are planning to launch in the future? Please describe in as much detail as possible. What problem are you trying to solve with the additional efforts and how will you measure success?

Yahoo! continues to work to address safety challenges using a multi-faceted approach. To that end, we continue to refine our internal technology for detecting illegal child pornography images, to target relevant safety messaging to the proper audience, to highlight our report abuse functionality to our users, to educate law enforcement on investigations involving Yahoo!, and to partner with our industry peers. Further, soliciting input and feedback from safety experts and participating in groups such as this one help us explore the efficacy of third-party safety products. A couple of examples of our continuing efforts include:

- As noted above, Yahoo! participates in the industry Coalition for Child Protection Technology ("Technology Coalition"). The members of the Technology Coalition are working on technologies such as applying hash value recognition to speed the detection and take down of images of apparent child pornography. In using this automated system, the Coalition members aim to deter the use of their systems by those who would trade in child pornography images and to speed takedown of such images in order to minimize potential exposure to users. Yahoo! is working with this group and NCMEC to help enhance our current capabilities for detecting child pornography images.
- In accordance with Yahoo!'s belief that educating all users about safe online practices is the first step in helping youth deal with online risks such as predators and bullying, Yahoo! plans to continue expanding its education and outreach efforts. For example, Yahoo! recently launched an online safety education video created in partnership with NCMEC's NetSmartz.org and aimed at educating teen users on managing their online reputations. We soon will be unveiling a second video to help teens understand how they can deal with cyberbullying. We anticipate that these will be the first in a series of youth-oriented efforts to provide our teen users with tips for protecting themselves from online risks. In addition, Yahoo! is adding new – and refining existing – online safety instructional materials for parents (available at safely.yahoo.com) in order to provide them with tools for teaching their children how to use Yahoo! products safely.

5. Based on what you've learned in trying to execute safety measures, what should the Technical Advisory Board know about dealing with actual implementation issues? What concerns do you have based on your own experiences? What are the strengths and weaknesses of implementing technical solutions?

There are many factors which impact whether technical solutions can be implemented across the Yahoo! network. First, any technical solution must be appropriate for the wide range of services that Yahoo! offers, as any implementation likely will impact users of email; small business services such as domains or web hosting; content services such as News, Travel, and Finance; as well as the community services that Yahoo! offers. Second, any solution must be capable of being implemented globally. A significant percentage of Yahoo!'s users live outside the United States.

Third, solutions must be able to scale to the size of Yahoo!'s network of 500 million users around the globe and do so with a high level of accuracy. Fourth, solutions must be low-cost or cost neutral, as Yahoo! is committed to continuing to offer users free access to basic core services such as email communications and important informational services such as News and Finance.

Finally, technical solutions need to be narrowly tailored to the safety issue that is to be solved and not interfere with legitimate users' online experiences.

Yahoo! has concerns about many of the technical solutions being discussed by the Task Force members. Many of the existing solutions are challenging because of the significant gaps in coverage both within the U.S. and outside, the burden placed on users in terms of financial cost and/or cost to privacy, and the lack of narrow tailoring to identified safety risks.

We're always open to technical solutions that focus on results, but no single technical solution will be the "silver bullet" that solves child online safety challenges. Yahoo! has developed (and continues to develop) a number of technical solutions within our own network of services. When we do so, however, we are very careful to design the solutions to focus on clearly inappropriate behavior or content and to implement solutions in a way that produces a minimum of interference with the legitimate use of our products and services.

In many cases, to be successful, a tool must be tailored both to the product where it will be deployed and to the specific type of problem it is trying to address. Examples of where we have developed useful tools to promote safety include our spam filters, sign-on seal, detection of malware and phishing URLs, reporting images of apparent child pornography, and various types of content moderation tools, such as reputation-based content moderation tools in properties like Answers and language filters for Chat and Message Boards. Given the success we've seen with our internally developed solutions, we believe that companies continuing to innovate on their own networks may be the best way to promote safety rather than trying to find a "one size fits all" solution.

Lastly, technical solutions must continue to be paired with other types of efforts to promote safety such as education and awareness, as well as assistance for law enforcement investigations and prosecutions.

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

**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 techn 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 _____ or John Morris at j_____



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>).

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 victimization². 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>



Family
Online Safety
Institute

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.



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)

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



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: 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

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

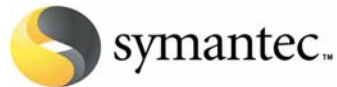


Sentinel Tech Holding Corp.: Statement Regarding the Internet Safety Technical Task Force's Final Report to the Attorneys General

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 a 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.



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 General, 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.

