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/istf

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

VI. Intellectual Property.

The Task Force has developed and posted an Intellectual Property Policy[2] 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

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, lending 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 perpetuated 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; Liau 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) ethnical 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 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, Philipe. 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 Pracising 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. Schmallenger, & 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 and 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, nonscalable 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 COrporation 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 lector 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 Intenet. 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 Langauge 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 Fllter
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. Verificage

APPENDIX E:

Submissions from Social Network Sites

Internet Technical Safety ~~Taskforce~~ – Request for Input
Bebo and AOL

Is this still around?

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

This whole report basically said nothing!

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 pro-active 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 (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
Director Member Services
Community Connect, Inc.
205 Hudson Street 6th Floor
New York, NY 10013
bsweeney@communityconnect.com
212-431-4477 ext. 238

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 out 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

COMMUNITY CONNECT INC.

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.

COMMUNITY CONNECT INC.

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.

COMMUNITY CONNECT INC.

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.safefamiles.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.

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.

205 HUDSON STREET, 6TH FLOOR, NEW YORK, NY 10013, TEL: 431-4477, FAX: 212-343-2410

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.

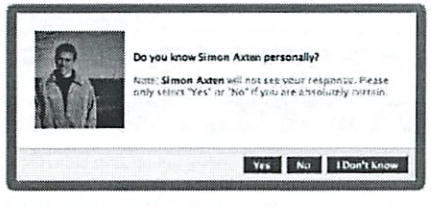
Relevant URLs: www.facebook.com
www.facebook.com/privacy
www.facebook.com/help.php

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.

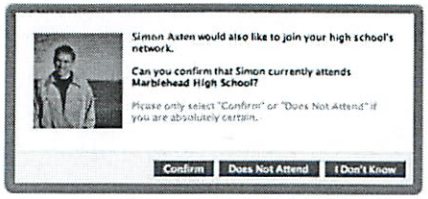
2. Facebook's network-based architecture strives to reflect as closely as possible real world social communities. By default, users' profiles are only available to those who share networks with them or have been confirmed as friends.

   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.

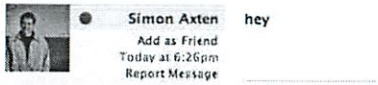


A high school network affiliation must be established through the process above before a user can gain access to the profiles of others on that network. Users must be 18 or under to join a high school network.



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.

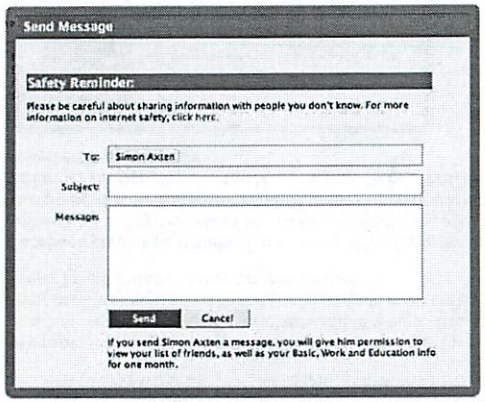
People who try to sign up with a birth date that makes them under 13 are blocked, and a persistent browser cookie is used to prevent further attempts at sign-up.

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.



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.

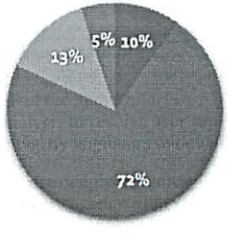
We are deeply committed to our own efforts in this area and believe the controls and processes we have built are leading the industry. At the same time, we recognize that protecting children online is an ongoing battle that requires cooperation among various groups, and we are always open to working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

3. 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.

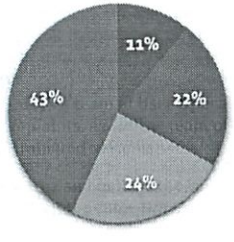
   We have also used our own Polling feature to gauge how minors are using the site, as well as how safe they feel on Facebook relative to other sites and the Internet at large. The results of a few of these polls, which use a sample of 500 users in the US aged 13-17, are below:

Have you ever seen nudity...

...on Facebook?



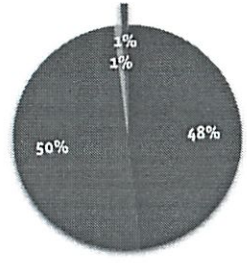
...on a website other than Facebook?



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.

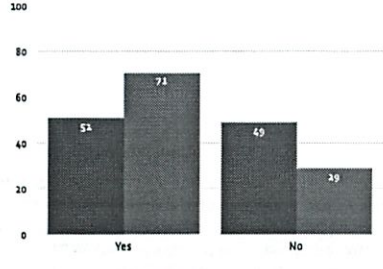
Do you know the people you interact with on Facebook in real life?



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.

Google

orkut

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.

Loopt, Inc.
www.loopt.com
590 W. El Camino Real
Mountain View, CA 94040

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.

FOX INTERACTIVE MEDIA

myspace.com
a place for friends

Safety | Security | Privacy **October 15, 2008**

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 <u>any</u> 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 it 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

FOX INTERACTIVE MEDIA

myspace.com
a place for friends

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

FOX INTERACTIVE MEDIA

myspace.com
a place for friends

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.

PSA:	***DONE***
MySpace and iKeepSafe Tutorials:	***DONE***
Parent Care Software:	***DONE***
Parent Care Hotline:	***DONE***
Parent Care Email:	***DONE***
Parent Guide:	***DONE***
New MySpace Safety Tips:	***DONE***

- 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/=

YAHOO!®

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.

at&t

December 17, 2008

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

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

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

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

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

December 21, 2008

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

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

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

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

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

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

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

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

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

Comcast

December 17, 2008

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

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

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

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

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

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

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

ConnectSafely
Smart Socializing Starts Here™
www.connectsafely.org

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

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

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

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

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

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

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

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

ENOUGH·IS·ENOUGH www.enough.org

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

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

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

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

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

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

Donna Rice Hughes, President, Enough Is Enough

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

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.

IDOLOGY INC.

December 17, 2008 – IDology, Inc

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

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

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

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

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

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

iKeepSafe

iKeepSafe Statement Regarding the ISTTF Final Report to the Attorneys General

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

Age Verification

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

a. We have no consistent and credible way to determine who is a ***custodial*** parent and who is a child. In today's Internet environment, this obstacle is insurmountable. (Would hospitals or county records clerks be asked to verify a birth parent? Is the birth parent still the legal guardian? Who determines eligibility? Will schools be asked to identify a custodial parent? Will a verification form, mailed or faxed from a residence determine parentage?)
b. Verifying children's ages will aggregate large databases of personal information of youth, creating problematic scenarios including commercial companies storing data on American children, identity risks, privacy concern, and substantial security risks. What happens when this database gets hacked?
c. It is important to note that many youth experience inappropriate contact and content, including home-produced pornography, *from other youth*. Age verification will not protect from these exposures.

Gaps in the Research

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

What Can Be Done Now

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

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

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

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

December 17, 2008

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

THE PROGRESS & FREEDOM FOUNDATION

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

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

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

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

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

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

December 17, 2008

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

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

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

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

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

--Chris Kelly, Chief Privacy Officer

facebook.

Address 156 University Avenue
Palo Alto, CA 94301
Telephone: 650 543.4800
Fax: 650 543.4801

Linden Lab

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

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

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

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

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

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

Microsoft

December X, 2008

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

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

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

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

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

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

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

myspace.com
a place for friends

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

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

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

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

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

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

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

Hemanshu Nigam, Chief Security Officer, MySpace

###

December 17, 2008

Institute for Policy Innovation
IPI

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

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.

symantec.

December 17, 2008

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

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

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

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

December 17, 2008

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

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

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

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

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

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

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

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

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

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

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

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

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

YAHOO!

December 17, 2008

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

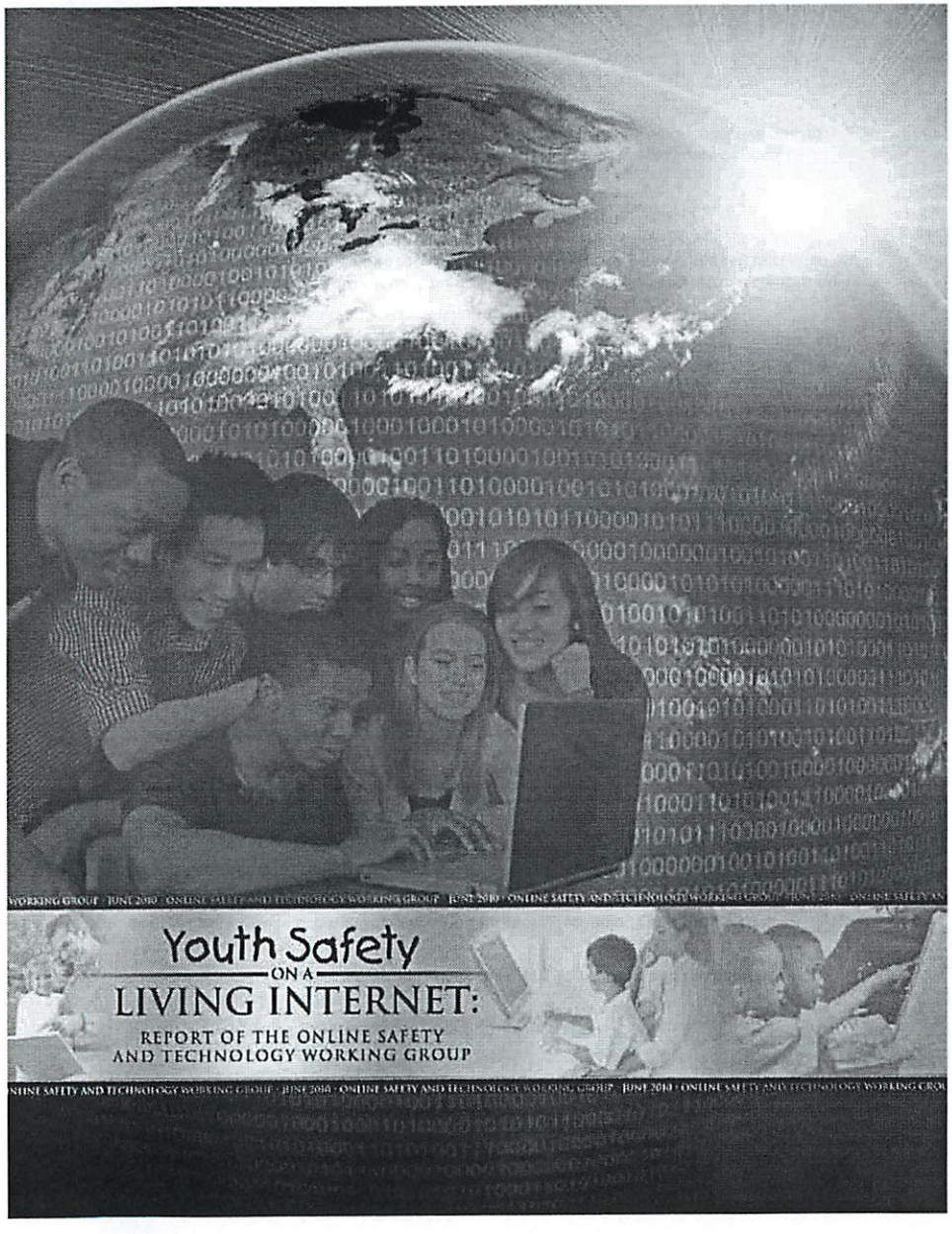
Yahoo! wishes to thank the Attorneys General, Berkman staff, and the task force participants for their hard work in developing a report that clarifies the risks currently facing children, and sheds light on the efficacy of existing technologies. We look forward to continuing our work with the state Attorneys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

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

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

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

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



2nd Report
For B teams
Read 9/12

YOUTH SAFETY ON A LIVING INTERNET:

REPORT OF THE ONLINE SAFETY AND TECHNOLOGY WORKING GROUP

JUNE 4, 2010

To: **The Honorable Lawrence E. Strickling**
Assistant Secretary of Commerce

The Honorable John D. Rockefeller IV, Chairman
Senate Committee on Commerce, Science and Transportation

The Honorable Kathryn Ann Bailey Hutchison, Ranking Member
Senate Committee on Commerce, Science and Transportation

The Honorable John F. Kerry, Chairman
Senate Commerce Subcommittee on Communications, Technology, and the Internet

The Honorable John Ensign, Ranking Member
Senate Commerce Subcommittee on Communications, Technology and the Internet

The Honorable Henry Waxman, Chairman
House Committee on Energy and Commerce

The Honorable Joe Barton, Ranking Member
House Committee on Energy and Commerce

The Honorable Rick Boucher, Chairman
House Commerce Subcommittee on Communications, Technology and the Internet

The Honorable Cliff Stearns, Ranking Member
House Commerce Subcommittee on Communications, Technology and the Internet

From: **Hemanshu Nigam**, Co-Chair
Online Safety and Technology Working Group

Anne Collier, Co-Chair
Online Safety and Technology Working Group

Date: June 4, 2010

On behalf of the Online Safety and Technology Working Group (OSTWG), we are pleased to transmit this report to you. As mandated, we reviewed and evaluated:

1. The status of industry efforts to promote online safety through educational efforts, parental control technology, blocking and filtering software, age-appropriate labels for content or other technologies or initiatives designed to promote a safe online environment for children;
2. The status of industry efforts to promote online safety among providers of electronic communications services and remote computing services by reporting apparent child pornography, including any obstacles to such reporting;
3. The practices of electronic communications service providers and remote computing service providers related to record retention in connection with crimes against children; and
4. The development of technologies to help parents shield their children from inappropriate material on the Internet.

The report contains recommendations in each of the above categories, as well some general recommendations. We believe these recommendations will further advance our collective goal to provide a safer online experience to our children.

We would like to personally thank the support of the National Telecommunications and Information Administration (NTIA) and its staff during this process. Their assistance throughout the past year was invaluable in allowing us to execute on our mandate. We would also like to recognize the leadership of our subcommittee chairs, Christopher Bubb, Larry Magid, Michael McKeehan, and Adam Thierer – each worked diligently to bring much consensus into the final report. We also want to thank the OSTWG members for the tremendous effort they put into their work all the while doing it in a most collaborative fashion. And finally, we would like to recognize the insight offered by representatives from the White House, the Department of Commerce, the Department of Education, the Department of Justice, the Federal Communications Commission, and the Federal Trade Commission.

As co-chairs we have been honored to have led the OSWTG on this journey, and we all look forward to working with you in bringing these recommendations to life – our nation's youth deserve no less.

////

THE ONLINE SAFETY AND TECHNOLOGY WORKING GROUP

CO-CHAIRS

Anne Collier
Co-Director
ConnectSafely.org
President
Net Family News, Inc.

Hemanshu Nigam
Founder
SSP Blue
Formerly Chief Security Officer
News Corporation

MEMBERS

Parry Aftab, Esq.
Founder and Executive Director
WiredSafety.org

Elizabeth Banker
Vice President and General Counsel
Yahoo! Inc.

Christopher Bubb
Assistant General Counsel, Public Safety and Criminal Investigations
AOL

Braden Cox
Policy Counsel
NetChoice Coalition

Caroline Curtin
Policy Counsel, Federal Affairs
Microsoft

Brian Cute
Vice President, Discovery Services
Afilias

Jeremy S. Geigle
President
Arizona Family Council

Marsali Hancock
President
Internet Keep Safe Coalition

Michael Kaiser
Executive Director
National Cyber Security Alliance

Christopher M. Kelly
Formerly Chief Privacy Officer and Head of Global Policy
Facebook

Brian Knapp
Chief Operating Officer
Loopt

Hedda Litwin
Cyberspace Law Counsel
National Association of Attorneys General

Timothy M. Lordan
Executive Director and Counsel
Internet Education Foundation

Larry Magid
Co-Director
ConnectSafely.org

Brian Markwalter
Vice President of Technology and Standards
Consumer Electronics Association

Michael W. McKeehan
Executive Director, Internet and Technology Policy
Verizon

Samuel C. McQuade III
Associate Professor
Rochester Institute of Technology

Orit H. Michiel
Vice President and Domestic Counsel
Motion Picture Association of America

John Morris
General Counsel
Center for Democracy and Technology

Jonathan Nevett
Vice President of Policy and Ethics
Network Solutions, LLC

Jill L. Nissen
Formerly, Vice President, Chief Policy Officer
Ning, Inc.

Jay Opperman
Senior Director of Security and Privacy
Comcast Corporation

Kevin Rupy
Director of Policy Development
USTelecom

John Shehan
Executive Director, Exploited Child Division
National Center for Missing and Exploited Children

Dane Snowden
Vice President, External and State Affairs
CTIA – The Wireless Association

Adam Thierer
President
Progress and Freedom Foundation

Patricia E. Vance
President
Entertainment Software Rating Board

Ralph James Yarro III
Founder, President, and CEO
Think Atomic, Inc.

FEDERAL GOVERNMENT REPRESENTATIVES

Paul R. Almanza
Deputy Chief
Child Exploitation and Obscenity Section
Criminal Division
Department of Justice

Robert Cannon
Senior Counsel for Internet Law
Office of Strategic Planning and Policy Analysis
Federal Communications Commission

Cheryl Petty Garnette
Director
Technology in Education Programs
Office of Innovation and Improvement
Department of Education

Nat Wood
Assistant Director
Division of Consumer and Business Education
Bureau of Consumer Protection
Federal Trade Commission

TABLE OF CONTENTS

EXECUTIVE SUMMARY

The Internet is a living thing. It mirrors and serves as a platform for a spectrum of humanity's lives, sociality, publications and productions. And as with all living things, its current state is guided and molded by the years of evolution it has gone through to reach its current place in our society. Tasked with the goal of examining the safety of this dynamic medium, the Online Safety and Technology Working Group (OSTWG) embraced its mission mindful of the great amount of work done before it. We approached our task with open eyes and open minds, while at the same time remaining aware of the many efforts that had gone before us, many of which individual OSTWG members had participated in. Still, we were determined to take our combined knowledge and insights gained over the past year to shed new light on the issues reflected in our recommendations to you.

The OSTWG was fortunate to have representatives from nearly every facet of the child online safety ecosystem represented. Members came from the Internet industry, child safety advocacy organizations, educational and civil liberties communities, the government, and law enforcement communities. Collectively, we brought to our work more than 250 years of experience in online safety from a spectrum of varying perspectives. We hope the set of recommendations we are delivering to you here will leave an indelible mark on the online experiences of our country's children as they evolve into adults in this digital century.

The OSTWG was established by the "Broadband Data Improvement Act" (the Act), Pub. L. No. 110–385. Section 214 of the Act, which was signed into law on October 10, 2008, mandated the NTIA to create the OSTWG, bringing this group together to focus on four different components of online safety.

Specifically, the OSTWG was established to review and evaluate:

- The status of industry efforts to promote online safety through educational efforts, parental control technology, blocking and filtering software, age-appropriate labels for content or other technologies or initiatives designed to promote a safe online environment for children;
- The status of industry efforts to promote online safety among providers of electronic communications services and remote computing services by reporting apparent child pornography, including any obstacles to such reporting;
- The practices of electronic communications service providers and remote computing service providers related to record retention in connection with crimes against children; and
- The development of technologies to help parents shield their children from inappropriate material on the Internet.

The Act specifies that the OSTWG must be comprised of up to 30 members who are "representatives of relevant sectors of the business community, public interest groups, and other appropriate groups and Federal agencies." This business community includes, at a minimum, Internet service providers, Internet content providers (especially providers of content for children), producers of blocking and filtering software, operators of social networking sites, search engines, Web portals, and domain name service (DNS) providers. Public interest groups may include organizations that work on behalf of children or study children's issues, Internet safety groups, and education and academic entities. The NTIA sought representatives from a broad spectrum of organizations to obtain the best information

available on the state of online safety. The OSTWG would also include representatives from various federal agencies. While federal agency members provided information and contributed to discussions at OSTWG meetings, the recommendations in this report do not necessarily represent the policy positions of the agencies or their leadership.

The full list of members is included in Appendix A. It is clear from the make-up of the OSTWG that the NTIA was successful in executing on this mandate of the Act. For that we are grateful, as it allowed for a multi-dimensional examination of the issues set before us.

OSTWG SUBCOMMITTEES

In order to provide you with a complete picture and set of recommendations in each of the areas outlined by the Act, we created a subcommittee for each topic put forth in the statute, each led by a subcommittee chair. Lawrence J. Magid led the Education subcommittee, Michael W. McKeehan led the Data Retention subcommittee, Christopher G. Bubb led the Child Pornography Reporting subcommittee, and Adam Thierer led the Technology subcommittee. Following an introductory meeting on June 4, 2009, we held meetings where each subcommittee invited experts to provide valuable insight to inform the work of that particular subcommittee. These meetings were held on September 24, 2009, November 3, 2009, February 4, 2010, and May 19, 2010. All meetings were held in Washington, D.C. and were open to the public and news media. The agenda for each of these subcommittee meetings is available in Appendix B as well as online on the Web.[1]

SPECIAL SPEAKERS

To build on the work of preceding task forces, give context to our work, and receive the most current thinking and research on youth Internet use, we invited a special guest to speak at each of our meetings. Here's a short summary of what each speaker said:

At our first meeting on June 4, 2009, Susan Crawford, JD, Assistant to the President for Science, Technology and Innovation and a member of the National Economic Council, called on this Group to focus on research-based education – of both parents and children – as a key to children's online safety. "I love this line, and I am going to repeat it: 'The best software is between the ears'," Crawford said. She asked us to "avoid the overheated rhetoric about risks to kids online," "insensitivity to the constitutional concerns that legitimize use of the Internet," and "one-size-fits-all solutions." She added that government does not have a very good track record with "technological mandates."

On September 24, 2009, Dr. Henry Jenkins, author and media professor at the University of Southern California, also cautioned us against sensationalist media coverage of digital teens. He said that what he and his fellow researchers of the $50 million McArthur Digital Youth Project have seen is that "most young people are trying to make the right choices in a world that most of us don't fully understand yet, a world where they can't get good advice from the adults around them, where they are moving into new activities that were not part of the life of their parents growing up – very capable young people who are doing responsible things, taking advantage of the technologies that are around them." Jenkins said teens are engaged in four activities "central to the life of young people in participatory culture: circulating media, connecting with each other, creating media, and collaborating with each other." It is crucial, he said, to bring these activities into classrooms nationwide so that all young people have equal opportunity to participate. This is crucial, too, because young people "are looking for

1 NTIA Web site (http://www.ntia.doc.gov/advisory/onlinesafety/)

guidance often [in their use of new media] but don't know where to turn," Jenkins told us. In focusing so much on blocking new media from school as a protection, schools are failing to do with today's media what they have long done for students with traditional media – enrich and guide their use. Finally, Jenkins asked us to take up "the ethics challenge" – creating the conditions for youth to absorb and learn in social-media projects and environments the kind of personal and professional ethics young people used to learn while working on high school newspapers.

"Digital ethics" was the focus of sociologist Carrie James's presentation at our November 3, 2009, meeting. Dr. James, research director at the Harvard University School of Education's GoodPlay Project, said, "There are also a lot of confused kids out there, some of them mal-intentioned perpetrators, but arguably more making naïve - and ethically ambiguous - choices that can hold serious ethical consequences." Seeming to reinforce Jenkins's observation at the previous meeting, she told us there is a dearth of ethical supports for youth in social media. More than 60% of GoodPlay's research sample named a parent, teacher or coach as a mentor or strong influence in their offline lives, but few adults were mentioned as guides in their social media use. Her research group found it "promising" that "nearly a third of the sample named a peer mentor" for their online experiences, but that's not promising, she said, "if ethical thinking is rare among peers online." With USC's New Media Literacies Project, the GoodPlay Project has released a casebook, *Our Space: Being a Responsible Citizen of the Digital World*, for educators focusing on two facets of ethics online, the latter having a great deal to do with online safety on the social Web: "Whether and how youth behave ethically themselves, and how they can protect themselves against unethical, irresponsible behavior of others."

The day before our February 4, 2010, meeting, Amanda Lenhart, senior research specialist at the Pew Internet & American Life Project, had released research on young people's use of the social Web, both fixed and mobile, finding that 93% of American teens (12-to-17-year-olds) use the Internet, 73% use social network sites, and 75% of them own cell phones. As for the newest tech-related risk to youth, so-called "sexting," Lenhart said at our meeting that her research had found that 4% of American teens have sent sexually suggestive images or videos of themselves via cell phone, and 15% have received such images from someone they know, with no gender differences in those percentages.

BACKGROUND & CONTEXT

The Internet, what we know about youth online risk, and the task of keeping online youth safe have all changed significantly in the 10 years since the COPA Commission reported to Congress.

From the perspective of today's increasingly user-driven multi-dimensional media environment, the task the COPA Commission was charged with what might today be considered a supremely simple one: to study "various technological tools and methods for protecting minors from material that is harmful to minors." At the time, however, during that "Web 1.0" era, when users were largely consumers rather than the producers, socializers, and communicators they have now become, examining potential solutions to even a single online risk, inappropriate content, seemed a big task.

So did that of the National Research Council, whose Computer Science and Telecommunications Board in 2002 conducted the study "Youth, Pornography, and the Internet."[2] Edited by former U.S. Attorney General Dick Thornburgh and Herbert S. Lin, the "Thornburgh Report" examined the issue of children's exposure to sexually explicit material online from multiple perspectives and reviewed a number of approaches to protecting children from encountering such material. The report concluded

2 "Youth, Pornography, and the Internet," Dick Thornburgh and Herbert S. Lin, editors, Computer Science and Telecommunications Board, National Research Council, 2002 (http://www.nap.edu/readingroom.php?book=youth_internet&page=index.html)

that "developing in children and youth an ethic of responsible choice and skills for appropriate behavior is foundational for all efforts to protect them – with respect to inappropriate sexually explicit material on the Internet as well as many other dangers on the Internet and in the physical world. Social and educational strategies are central to such development, but technology and public policy are important as well – and the three can act together to reinforce each other's value." The report encapsulated this finding into the oft-quoted and succinct "swimming pool analogy," acknowledging the protective value of fences around pools while asserting that such "technology" could never replace the life-long protection of teaching kids how to swim.

Fast-forward six years to the next national youth-online-safety task force, that of Harvard University Law School's Berkman Center for Internet & Society, assembled in 2008 and officially called the Internet Safety Technical Task Force (ISTTF). In the highly charged Net-safety climate of that time, fears of predators in a "new phenomenon" called social networking sites were running high among parents and policymakers alike. The ISTTF, too, was charged with a more specific task than ours: examine the state of online identity-authentication technology and other online safety tools that would inform online safety for minors on the social Web. The charge, however, implied a prescribed solution that had not had the benefit of a thorough diagnosis. Consequently, in addition to a review of current age-verification products and technologies, the Internet Safety & Technical Task Force, wisely undertook a comprehensive review of academic research on youth risk online up to 2008.

The ISTTF's top two findings[3] – that "sexual predation on minors by adults, both online and offline, remains a concern" but that "bullying and harassment, most often by peers, are the most frequent threats that minors face, both online and offline" – point not just to the OSTWG's challenge but that of anyone charged with analyzing online safety solutions today – the need for better questions, based on a greater understanding of the nature of the Internet today and how youth use it.

What these two findings on the part of the ISTTF suggest is not only that, thanks to the growing body of youth-online-risk research, we are now able to seek solutions as a society which are fact-based, not fear-based, but also that minors themselves – mainly pre-teens and teens (though the tech-literacy age is going down) – have a role to play in improving their own safety online and that of their peers.

For example, the ISTTF found that "many of the threats that youth experience online are perpetrated by their peers, including sexual solicitation and online harassment." The report also cited more than a dozen times a 2007 study published in Archives of Pediatrics & Adolescent Medicine[4], which found that "youth who engage in online aggressive behavior ... are more than twice as likely to report online victimization."

It is clear, then, that the definition of "youth online safety" has broadened and become more complex in the past 10 years, as have the role of the online user and the inter-connected devices today's user takes advantage of when consuming, socializing, producing, and connecting. In addition to cyberbullying, inappropriate content, and predation, other risks have emerged, including "sexting" and the risks related to geolocation technology in online applications and on mobile phones. Thus, we are forced to either create a new taxonomy of online safety, or at the very least, expand our historical definition. While many possibilities exist – simply to make the point more obvious – here is one

3 "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," the Berkman Center for Internet & Society at Harvard University, December 31, 2008 (http://cyber.law.harvard.edu/sites/cyber.law.harvard.edu/files/ISTTF_Final_Report-Executive_Summary.pdf)

4 "Internet Prevention Messages: Targeting the Right Online Behaviors," by Michele L. Ybarra, Kimberly J. Mitchell, David Finkelhor, and Janis Wolak, Archives of Pediatrics & Adolescent Medicine, February 2007 (http://archpedi.ama-assn.org/cgi/content/full/161/2/138)

example of a taxonomy focused less on specific technologies or devices and more on the categories of safety desired:

- **Physical safety** – freedom from physical harm
- **Psychological safety** – freedom from cruelty, harassment, and exposure to potentially disturbing material[5]
- **Reputational and legal safety** – freedom from unwanted social, academic, professional, and legal consequences that could affect users for a lifetime
- **Identity, property, and community safety** – freedom from theft of identity & property

This in no way diminishes the importance of any single form of safety, but it does demonstrate the complexity of our task as a society to ensure young people's safety on the fixed and mobile Internet. And, because of the key role young people increasingly play in their own safety online, it also points to the growing importance of online citizenship and media-literacy education, in addition to what has come to be seen as online safety education, as solutions to youth risk online.

Other important factors that need to be considered by any task force or working group present and future:

- There's no one-size-fits-all, once-and-for-all solution to providing children with every aspect of online child safety. Rather, it takes a comprehensive "toolbox" from which parents, educators, and other safety providers can choose tools appropriate to children's developmental stages and life circumstances, as they grow. That toolbox needs to include safety education, "parental control" technologies such as filtering and monitoring, safety features on connected devices and in online services, media ratings, family and school policy, and government policy. In essence, any solution to online safety must be holistic in nature and multi-dimensional in breadth.
- To youth, social media and technologies are not something extra added on to their lives; they're embedded in their lives. Their offline and online lives have converged into one life. They are socializing in various environments, using various digital and real-life "tools," from face-to-face gatherings to cell phones to social network sites, to name just a few.
- Because the Internet is increasingly user-driven, with its "content" changing in real-time, users are increasingly stakeholders in their own well-being online. Their own behavior online can lead to a full range of experiences, from positive ones to victimization, pointing to the increasingly important role of safety education for children as well as their caregivers. The focus of future task forces therefore needs to be as much on protective education as on protective technology.
- The Internet is, in effect, a "living thing," its content a constantly changing reflection not only of a constantly changing humanity but also its individual and collective publications, productions, thoughts, behaviors, and sociality.

Based on this "snapshot" of the Internet as we are experiencing it right now, the best solutions for promoting child safety, security, and privacy online must be the result of an ongoing negotiation involving all stakeholders: providers of services and devices, parents, schools, government, advocates, healthcare professionals, law enforcement, legislators, and children themselves. All have a role and responsibility in maximizing child safety online.

5 We chose the term "disturbing" to signify a broad and encompassing meaning that includes what could be disturbing when viewed by a minor and what parents may consider to be disturbing for their own children. We did not use the term "harmful," given its more narrowly defined meaning that has resulted from legal court opinions and its use in federal statutes.

SUMMARIES OF THE SUBCOMMITEE REPORTS

In order to fully grasp the breadth and depth of the findings and recommendations of the four subcommittees, it is important to read the full report of each subcommittee in the body of this document. The following only briefly summarizes their findings and recommendations.

SUBCOMMITTEE ON INTERNET SAFETY EDUCATION

Summary

In the late '90s, experts advised parents to keep the family Internet connected computer in a high-traffic part of the house, but now parents must account for Internet access points built into many digital devices, including cell phones. Research has told us that many of the early significant concerns regarding children and their use of the Internet, such as predation, exist but not nearly in the prevalence once believed. Other risks, such as cyberbullying, are actually much more common than thought – starting as early as 2nd grade for some children. Meanwhile, "new" issues such as "sexting" garner a great deal of media attention, though recent studies suggest it is not quite as common as initially believed. Given all the above and the finding of the preceding task force (the ISTTF) that not all youth are equally at risk, it now seems clear that "one size fits all" is not a good strategy. Instead, a strong argument can be made for applying the Primary/Secondary/Tertiary model used in clinical settings and risk-prevention programs to Internet safety. This "levels of prevention" method would represent a tailored and scalable approach and factor in the high correlation between offline and online risk. The approach would also work in concert with non-fear-based, social-norms education, which promotes and establishes a baseline norm of good behavior online.

Research also shows that civil, respectful behavior online is less conducive to risk, and digital media literacy concerning behavior as well as consumption enables children to assess and avoid risk, which is why this subcommittee urges the government to promote nationwide education in digital citizenship and media literacy as the cornerstone of Internet safety.

Industry, NGOs, schools, and government all have established educational strategies; however effectiveness has not been adequately measured. At the federal level, while significant progress has been made with projects such as OnGuardOnline and NetCetera, more inter-agency coordination, public awareness-raising, and public-/private-sector cooperation are needed for national uptake in schools and local communities.

Recommendations

- Keep up with the youth-risk and social-media research, and create a web-based clearinghouse that makes this research accessible to all involved with online safety education at local, state, and federal levels.
- Coordinate Federal Government educational efforts.
- Provide targeted online-safety messaging and treatment.
- Avoid scare tactics and promote the social-norms approach to risk prevention.
- Promote digital citizenship in pre-K-12 education as a national priority.
- Promote instruction in digital media literacy and computer security in pre-K-12 education nationwide.

- Create a Digital Literacy Corps for schools and communities nationwide.
- Make evaluation a component of all federal and federally funded online safety education programs (evaluation involving risk-prevention expertise).
- Establish industry best practices.
- Encourage full, safe use of digital media in schools' regular instruction and professional development in their use as a high priority for educators nationwide.
- Respect young people's expertise and get them involved in risk-prevention education.

SUBCOMMITTEE ON PARENTAL CONTROLS & CHILD PROTECTION TECHNOLOGY

Summary

There is no quick fix or "silver bullet" solution to child safety concerns, especially given the rapid pace of change in the digital world. A diverse array of protective tools are currently available today to families, caretakers, and schools to help encourage better online content and communications. They are most effective as part of a "layered" approach to child online safety. The best of these technologies work in tandem with educational strategies, parental involvement, and other approaches to guide and mentor children, supplementing but not supplanting the educational and mentoring roles. These products and services need to be designed with the needs of families in mind, being easy to use, accessible, flexible, and comprehensible for the typical parent. Industry should assist by continuing to formulate and refine best practices and self-regulatory systems to empower users with more information and tools so that they can make appropriate decisions for themselves and their families, including product settings that are defaulted in a thoughtful way. Government should avoid rigid, top-down technological mandates and instead enhance funding and encourage collaborative, multi-faceted, and multi-stakeholder initiatives and approaches to enhance online safety via innovation and cooperation.

Recommendations

- Engage in ongoing awareness-building efforts.
- Promote greater transparency for parents as to what sort of content and information will be accessible and recorded with a given product when their children are online.
- Bake parental empowerment technologies and options possible into product development whenever possible.
- Develop a common set of terms, agreed upon by the industry, across similar technologies.
- Promote community reporting and policing on sites that host user-generated content.

SUBCOMMITTEE ON CHILD PORNOGRAPHY REPORTING

Summary

Though mandated to study 42 U.S.C. § 13032, that section was repealed almost immediately after the mandate, and, accordingly, this subcommittee endeavored to compare and contrast § 13032 with its de facto replacement, now codified in 18 U.S.C. §§ 2258A through 2258D via the PROTECT Our

Children Act of 2008. Although § 13032 was a significant step forward in requiring service providers to report apparent child pornography when discovered, it lacked specificity in several key areas, including what additional information relating to the reported content would be valuable for law enforcement and whether any explicit criminal immunity would be granted to service providers who were implicitly tasked with transmitting potentially illegal images to the National Center for Missing and Exploited Children (NCMEC). As service providers as well as NCMEC, law enforcement, and prosecutors gained experienced under § 13032, its shortcomings became even more apparent. Service providers were concerned with the legal implications of transmitting illegal material and, without statutory guidance, law enforcement was often not receiving enough useful information from providers to push investigations forward. Sections 2258A *et seq.* improved on the previous provision by explicitly detailing the types of information service providers could include in a report, granting NCMEC more operational flexibility to route reports received, increasing fines, limiting liability for service providers both criminally and civilly, and quite creatively requiring providers to treat NCMEC's notification of receipt of a report as a request to preserve relevant subscriber information. The Act appears to have had a near instant impact on the volume of reports received by NCMEC, which recorded an increase of 84% from 2008-2009 and, at the time of this report, were on pace for an increase of 78% from 2009-2010.

Recommendations

- Task the appropriate executive agency with the objective to conduct a survey using an empirically reliable method to assess industry efforts to promote online safety by means of the new reporting provisions of § 2258A.
- Encourage outreach by NCMEC, government agencies, advocacy groups, and service providers to promote increased awareness of the PROTECT Our Children Act through education, information sharing efforts, and the establishment of sound practices for reporting and data preservation.
- Encourage nascent or smaller service providers who may lack the necessary networking contacts or experience to seek out meetings with NCMEC and law enforcement concerning the reporting and preservation provisions of the Act.
- Continue to encourage collaboration and information sharing among providers to develop new technologies that disrupt the transfer of online child pornography and facilitate reporting to NCMEC.
- Consider tax credits or other financial incentives to assist service providers in bearing the development and implementation costs associated with securely retaining data outside the course of normal business.
- Consider incentives for service providers to establish wellness programs for the employees who face the task of reviewing disturbing images of child sexual abuse in order to maintain compliance with the mandatory reporting requirements.

SUBCOMMITTEE ON DATA RETENTION

Summary

Data retention is a very contentious subject from a policy angle, fraught with conflicting needs and concerns from the perspective of the three groups represented in this report: law enforcement, industry, and consumer privacy. While law enforcement understands the need to carefully consider

all sides of the issue, they postulate that mandatory data retention sufficient to facilitate the effective investigation of online crimes is ultimately workable and will allow law enforcement to solve more crimes involving the sexual exploitation of children. From the industry perspective, while the cost of data storage has drastically fallen over the years, the true cost of retaining data comes in the form of having to protect ever increasing amounts of end users' private data from smarter and smarter criminals lurking on the Internet. Further assessment of the data preservation features enacted in the PROTECT Our Children Act, industry suggests, should occur before considering mandatory data retention. The consumer privacy perspective offers that in addition to issues regarding free speech, mandatory data retention would be overly broad in that it would cover legitimate users and bad actors alike, would be accessible by subpoena without judicial oversight in many situations, and would create a highly valuable database target for information thieves. In the end, it is about striking a balance between law enforcement's legitimate need to investigate and prosecute crimes against children facilitated by the Internet, end-users' legitimate privacy expectations, and the burden of data storage costs to ISPs and OSPs and their subsequent ability to operate as a business.

Recommendations

- ISPs and OSPs should have regular meetings and engage ICAC task forces and federal law enforcement agencies to cross-train on emerging threats, resolve operational glitches, and develop a set of evolving practices and procedures.
- Privacy concerns regarding vast amounts of stored data must be addressed.
- If they are to occur, data retention debates should happen at the federal level, so as not to add further confusion concerning competing regulations among states.
- Congress should assess the results of the data preservation procedures enacted in the PROTECT Our Children Act before considering mandatory data retention.
- We encourage you to read the full subcommittee reports contained in this document to grasp fully not only the insight contained in them, but also the twenty-six (26) recommendations we have provided.

RECOMMENDATIONS FROM THE CO-CHAIRS

Each of the Online Safety & Technology Working Group's four subcommittees have provided recommendations specific to the statute's requirements. As co-chairs, we had not only the honor of guiding a congressionally mandated working group, but also the challenges that come with such a task. We feel it is important for us to provide some of our learned insight to future task forces that will no doubt follow the OSTWG. With this in mind, we urge Congress to consider a few general recommendations concerning the overall mission of child online safety going forward:

1. **Provide proper support to task forces.** When creating future task forces, we recommend that legislation fully empower the appointed group to accomplish the task with which it's charged. Any congressionally mandated cross-sector child safety panel needs to be backed by the resources needed to succeed – sufficient time, if constrained as we were by the Paperwork Reduction Act, and sufficient resources, such as funds for travel by members and speakers and funds for meeting accommodations and staff support. An unfunded mandate creates obstacles that can easily distract from the great work that such mandates can lead to by placing undue burdens on the citizens called upon to serve the American public.

2. **Fill the prescription.** We have completed the work the statute required, but we suggest that there be follow-through. A report is half the job. Now fill the prescription, taking up or studying the value of all the recommendations in this report and determining a course of action. In order to do this, you might consider another congressional mandate that creates the group or groups to take up this important task.
3. **Create a coordinating body.** Although part of a single administration, government agencies can have different (and sometimes conflicting) views and philosophies concerning approaches to addressing many topics. Especially in the area of online child protection, industry can find itself challenged by these differing or even contending government agencies. We recommend the formation of a sufficiently funded, cross-functional group – representing key government agencies, industry, and NGOs – to help build consensus and coordinate efforts across the sectors.
4. **Review, identify, then publicize federal programs.** Conduct a full review of all child online safety projects and programs the federal government has undertaken. Evaluate these for success and then widely promote outstanding projects, such as Net Cetera and Admongo.gov, as opportunities for public/private sector partnerships in online risk prevention. Then promote the creation of these partnerships.
5. **Take a multi-stakeholder approach.** On any topic concerning today's complex new media environment – from education to law enforcement to parenting to risk prevention – no single stakeholder can represent all the expertise needed. As we said at the beginning, the Internet is a living thing reflecting all of life and, where children are concerned, that includes a spectrum of issues – from learning, child development, sociality, and entertainment at one end to crime and victimization at the other. Please recognize this reality and draw upon diverse expertise in all policymaking.

CONCLUSION

Any report about both the Internet and children is necessarily a freeze frame of a rapidly moving landscape – not only because both the technology and how children use it change so quickly but also because of the rapidly growing bodies of youth-risk and social-media research. Thus, any recommendations about children's online safety must take into account the dynamic nature of this landscape. The OSTWG has attempted to offer recommendations that will stand the test of time by stressing that lawmakers, government, and risk-prevention practitioners rely heavily on the research, as it unfolds, to get an accurate picture of what needs to be addressed when it is being addressed. This is in no way dissimilar to the approach policymakers have taken with our nation's longest living laws and policies, which continue to stand up to historical, behavioral, and technological change.

In closing, we stress once again that in order to fully comprehend the significance of the recommendations OSTWG makes, it is critical to read the entire report. We hope that as law and policy makers do so and continue to factor in an even broader spectrum of expertise than the OSTWG already represents, we will begin as a society the process of figuring out and filling the right prescription for child safety online.

SUBCOMMITTEE ON INTERNET SAFETY EDUCATION

To understand how industry, schools, non-profits and government can best provide Internet safety education, we must first grapple with what it is we're educating about and then tackle how to go about the business of educating. And to do that we need to understand the risks and the way youth actually use the Internet and the social media they access through computers, mobile phones, game consoles and other devices.

A lot has changed since the last major congressionally mandated look at Internet safety. When the Commission on Online Child Protection (COPA) issued its Report to Congress in 2000, there were no social networking sites, cell phones were pretty much limited to making phone calls and the primary perceived risks associated with the Internet were access to pornography and other inappropriate material and the fear of adult predators using the Net to entrap our children. In 2000, "place the computer in a central area of the house" was good advice. But that was before Netbooks, tablets, web-enabled smart phones, Wi-Fi and wide-area wireless networks.

There have also been profound changes in the way young people use technology.
In the ensuing decade, young people's use of the Net has shifted away from being mostly consumers of information to becoming active participants. Social networking and video sites have empowered young people not only to shape their own lives but have a direct impact on the media landscape that affects themselves, their peers and adults as well. In February, 2010, the Pew Internet & American Life Project reported[6] that "73% of wired American teens now use social networking websites," up from 55% two years earlier.

Young people have also gravitated toward mobile devices enabling them to do far more than talk. A 2010 Nielsen study[7] on teen use of text messaging found that American teens send and receive an average of 3,146 text messages a month.

PREDATOR DANGER

Knowing that young people spend a considerable amount of time "hanging out" online, many caring adults – including elected officials – naturally worry that they are at risk from predators that might in some way harm them. And, indeed, there are examples of sting operations by law enforcement (and famously even TV crews) that have been successful in exposing adult "predators" who have made online sexual advances to undercover officers and other adults posing as children and teens. To the extent that young people have received an unwanted sexual solicitations online, data from a 2000 DOJ-funded study and a 2006 follow-up from the Crimes Against Children Research Center (CACRC) at the University of New Hampshire concluded that "youth identify most sexual solicitors as being other adolescents."

That is not to say that unwanted solicitations, whether from an adult or a minor, can't have serious consequences, but studies – including some funded by the U.S. Department of Justice – have shown

6 Pew Internet & American Life Project: Social Media and Young Adults (http://www.pewinternet.org/Reports/2010/Social-Media-and-Young-Adults.aspx?r=1)

7 Nielsenwire: Under-aged Texting: Usage and Actual Cost (http://blog.nielsen.com/nielsenwire/online_mobile/under-aged-texting-usage-and-actual-cost/)

that the statistical probability of a young person being physically assaulted by an adult who they first met online is extremely low.

In a report published in the February/March 2008 issue of *American Psychologist*[8], researchers from CACRC found that "adolescents' use of popular social networking sites such as MySpace and Facebook do not appear to increase their risk of being victimized by online predators. Rather, it is risky online interactions such as talking online about sex to unknown people that increases vulnerability, according to the researchers."

After reviewing peer-reviewed studies, the Berkman Center's Internet Safety Technical Task Force[9] (the "Task Force") last year found that "cases [of adult to child sexual encounters on social networks] 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 also concluded that "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." In its review of the youth-risk literature, the Task Force's Research Advisory Board, made up of distinguished scholars and experts in the field of youth safety, concluded, "Youth identify most sexual solicitors as being other adolescents (48%; 43%) or young adults between the ages of 18 and 21 (20%; 30%) and that youth typically ignore or deflect solicitations without experiencing distress."

CYBERBULLYING

What the Task Force and many researchers did find was that "bullying and harassment, most often by peers, are the most frequent threats that minors face, both online and offline."

"Cyberbullying, as it is called when youth are bullied via computers or mobile phones, is real and is affecting a statistically significant number of American youth. And it can start "as early as the 2nd grade for some children," according to a study conducted by Rochester Institute of Technology.[10]
The actual percentage is difficult to pin down, but a 2008 Centers for Disease Control (CDC) *Electronic Media and Youth Violence* issue brief[11] reported that "9% to 35% of young people say they have been the victim of electronic aggression."

Among certain populations the problem is even worse. A study conducted at Iowa State University by Warren Blumenfeld and Robyn Cooper[12] found that 54% of lesbian, gay, bisexual and transgender (LGBT) youth had been victims of cyberbullying within the past 30 days. Forty-five percent of the respondents "reported feeling depressed as a result of being cyberbullied," according to the study's authors. Thirty-eight percent felt embarrassed, and 28% felt anxious about attending school. The authors reported that "more than a quarter (26%) had suicidal thoughts."

NOT ALL AGGRESSIVE BEHAVIOR RISES TO THE LEVEL OF BULLYING

The Centers for Disease Control defined electronic aggression as "any type of harassment or bullying (teasing, telling lies, making fun of someone, making rude or mean comments, spreading rumors,

8 University of New Hampshire Crimes Against Children Research Center: Internet Predator Stereotypes Debunked in New Study (http://www.unh.edu/news/cj_nr/2008/feb/fw18internet.cfm)

9 Internet Safety Technical Task Force: Enhancing Child Safety and Online Technologies (http://cyber.law.harvard.edu/pubrelease/isttf/)

10 Rochester Institute of Technology: A Survey of Internet and At-risk Behaviors (http://www.rtcsel.org/RIT%20Cyber%20Survey%20Final%20Report.pdf)

11 Electronic Media and Youth: A CDC Issue Brief (http://www.cdc.gov/violenceprevention/pdf/EA-brief-a.pdf)

12 Iowa State researchers publish national study on cyberbullying of LGBT and allied youths (http://www.news.iastate.edu/news/2010/mar/cyberbullying)

or making threatening or aggressive comments) that occurs through email, a chat room, instant messaging, a website (including blogs), or text messaging." This is a broader spectrum of behavior than researchers' definition of cyberbullying, which generally refers to unwanted aggression that is repeated over time with an imbalance of power between the perpetrator(s) and the victim (see also the *Journal of Adolescent Health, August 2007*.[13] Others define it as repeated unwanted harassment, or a one-time serious threat of bodily harm such as "I will kill you!", which mirrors many state harassment law approaches.

Cyberbullying is basically the same as real-world bullying, though it has elements that don't exist in the physical world such as anonymity, the ability to impersonate the victim, follow the victim home, embarrass the victim in front of an unseen (and potentially vast) online audience and persist online over a long period of time. Also, cyberbullying is typically psychological rather than physical and it's possible for the bully to remain anonymous. But there is often a link between cyberbullying and real-world bullying. In a 2008 cyberbullying study[14] of middle school students conducted by Sameer Hinduja and Justin Patchin, 82% said that the person who bullied them via technology was either from their school (26.5%), a friend (21.1%), an ex-friend (20%) or an ex-boyfriend or ex-girlfriend (14.1%).

A 2009 study[15] carried out by Harris Interactive on behalf of Cox Communications in partnership with the National Center for Missing & Exploited Children and John Walsh found that approximately 19% of teens say they've been cyberbullied online or via text message and that 10% say they've cyberbullied someone else. The Cox study defined cyberbullying as "harassment, embarrassment, or threats online or by text message," which is actually more consistent with the CDC's definition of "electronic aggression" than with the classical definition of bullying.

While the study didn't address the issue of cyberbullying, there is evidence that overall physical bullying is on the decline. Writing in the *Archives of Pediatrics and Adolescent Medicine*[16], David Finkelhor, Heather Turner, Richard Ormrod, and Sherry Hamby found that 15% of youth (ages 2-17) reported that they were physically bullied in 2008. The good news is that that percentage went down from 22% in 2003. The study also found that the percentage reporting a sexual assault decreased from 3.3% to 2%. Lead author Finkelhor noted that declines in bullying and sexual assault and that these problems have been aggressively targeted by school programs and other prevention efforts in recent years. "This suggests that some of the decline may be the fruits of those programs," he said.

"SEXTING"

There is a lot of concern about young people using cell phones and computers to distribute naked or sexually suggestive pictures of themselves, a practice that recently came to be known as "sexting." Estimates of the extent of the problem have varied widely, but a recent study by the Pew Internet & American Life Project[17] "found that 4% of cell-owning teens ages 12-17 say they have sent sexually suggestive nude or nearly nude images or videos of themselves to someone else via text messaging." Fifteen percent of young respondents "say they have received such images of someone they know via text message."

13 Does Online Harassment Constitute Bullying? An Exploration Of Online Harassment by Known Peers and Online-Only Contacts (http://unh.edu/ccrc/pdf/CV172.pdf)

14 Cyber Bullying Research Center (http://www.cyberbullying.us/research.php)

15 Survey: Teens 'sext' and post personal info. News.com (http://news.cnet.com/8301-19518_3-10272311-238.html)

16 *Archives of Pediatric and Adolescent Medicine:* "Trends in Childhood Violence and Abuse Exposure" (http://www.unh.edu/ccrc/pdf/CV196.pdf)

17 Pew Internet & American Life Project: "Teens and Sexting" (http://www.pewinternet.org/Press-Releases/2009/Teens-and-Sexting.aspx)

While 4% who admit having sent a "sext" is still a large number, it's far from the 20% figure reported in a less rigorous 2009 study that prompted a major news website to write in a headline, "Sexting Shockingly Common Among Teens."[18]

As we look at the sexting data, it's important to try to view the issue from the perspective of teens. There are certainly teens who have been strongly affected by sexting. *Sexting in America*, a documentary[19] created for MTV's A Thin Line Campaign in February, 2010 depicted sexting's impact on two teens. One teen named Ally was extremely distraught after a picture she sent to an ex-boyfriend was distributed all over school. Another teen, Philip Albert, is suffering the legal consequences of having sent out naked pictures of his 16-year-old girlfriend in a fit of anger in the middle of the night. She took and sent him the photos when he was 17, but he distributed them a month after his 18th birthday, which resulted in criminal charges. He's now on probation and, unless his lawyer is successful in getting the court to take him off the list, he could remain on the registered sex offender list until age 43. He told MTV that he was kicked out of college, can't find work, and he can't live with his father because his dad lives near a school.

CONSEQUENCES OF SEXTING

One interesting set of findings from that 2008 Cox study is that 90% of youth who admitted that they "sent a sext" reported that nothing bad happened as a result. Two percent said that they got in trouble after the photo was forwarded to an "authority figure"; only 1% said the photo was posted online; 2% said the person they sent the photo to made fun of them; 2% said the photo was forwarded to someone they didn't want to see it; and 4% said the person they sent the photo to threatened to send it to someone else. The study found that 14% of "sexters" said they were caught by parents (9%), a teacher (1%), another authority figure (3%) or someone else (3%)

Though most incidents of sexting never make it to legal authorities and, even when they do, most police and prosecutors are using their discretion to deal with the cases without resorting to criminal prosecution, there have been some cases where minors have been arrested, tried and convicted of manufacturing, possessing and/or distributing illegal child pornography. Some States are addressing the issue by decriminalizing the voluntary taking, possession and consensual sharing of sexual or nude images between minors. Recently, some courts have addressed the use of child pornography and sex offender laws in sexting cases, chastising over-zealous prosecutorial actions.

The National Center for Missing & Exploited Children's Policy Statement on Sexting[20] provides advice to law enforcement on what is and is not sexting and how to approach individual cases. "NCMEC," according to the policy, "does not believe that a blanket policy of charging all youth with juvenile or criminal violations will remedy the problem of sexting."

The Youth Online Safety Working Group (YOSWG) which consists of several law enforcement, child protection and education organizations and agencies, has developed an "Interdisciplinary Response to Youth Sexting" for educational professionals and law enforcement. The document recommends, among other things, that authorities "recognize possible causes of sexting within schools by examining school climate and any underlying behavioral issues" and that they "use discretion when

18 "Sexting Shockingly Common Among Teens" at CBSNews.com (http://www.cbsnews.com/stories/2009/01/15/national/main4723161.shtml)

19 MTV Documentary: *A Thin Line* (http://www.athinline.org/)

20 The National Center for Missing & Exploited Children: Policy Statement on Sexting (http://www.missingkids.com/missingkids/servlet/NewsEventServlet?LanguageCountry=en_US&PageId=4130)

What are they trying to stop

determining legal actions." YOSWG is also recommending prevention education programs for educators and law enforcement and is encouraging a "team approach" to "combat the problem of sexting."[21]

INAPPROPRIATE CONTENT

The report of our Sub-Committee on Parental Controls Technologies deals extensively with the issue of inappropriate content, but there is also an educational component to this issue. In addition to all of the child-friendly material online, there are some websites that contain material that most would agree can be harmful or at least disturbing to children.

These include sites that depict sexual content as well as those that encourage hate speech, violence or unsafe activities such as drinking, drug use or eating disorders. With some exceptions (such as child pornography, obscenity and sites that advocate violence against individuals), this material is constitutionally protected and any efforts to keep children from seeing it must be balanced with the rights of adults to produce and consume such material.

At its September meeting, the Working Group heard from Jessica Gonzales of the National Hispanic Media Coalition and Steve Sheinberg from the Anti-Defamation League about the impact of hate content on youth. Ms. Gonzales warned of the harmful impact of online "speech that induces encourages or otherwise legitimizes violence against particular groups of people, that … truly crosses the line or dances very close to the line of unprotected speech." Mr. Sheinberg agreed but observed (speaking for the ADL) that "We believe that the best antidote to hate, to hate speech is more speech – is good speech."

While, in most cases, there is nothing government can do to take down such material, there are ways that government can help parents in their own efforts to both shield their children from such material and help their children more effectively deal with it when they do encounter it. This includes education on the availability and use of parental control tools and encouraging instruction in critical thinking and media literacy – helping children understand how to make good decisions when selecting material for consumption and processing material that they see. It also includes helping parents better understand the actual impact of inappropriate material, which varies greatly based on the material itself, the maturity of the child and the extent of exposure, for example occasional exposure versus obsessive interest in certain types of sexual content.

OTHER RISKS

There are other risks children face online. In his introduction to "A Broadband Plan for Children and Families"[22] this March, Federal Communications Commission Chairman Julius Genachowski talked about "Harmful Websites," pointing out that "35% of eating disorder patients visit pro-anorexia websites." He also discussed distracted driving, citing data that "a quarter of U.S. teens with cell phones say they have texted while driving," an activity that can clearly lead to death or serious injury. He also discussed "Inappropriate Advertising" that exposes young people to potentially unhealthy or inappropriate messages such as ads for male enhancement drugs or sugary foods. These, along with access to online pornography, hate sites, and many other problem areas related to the Information Age are a constant challenge for young people.

21 "Interdisciplinary Response to Youths Sexting" (http://www.oakland.k12.mi.us/LinkClick.aspx?link=SafeSchools%2FInterdisciplinary+Response+to+Youths+Sexting.pdf&tabid=656&mid=3640)

22 FCC's Broadband Plan for Children and Families (http://hraunfoss.fcc.gov/edocs_public/attachmatch/DOC-296829A1.pdf)

SECURITY RISKS AND IDENTITY THEFT

Young people, along with the rest of us, are also exposed to spam, malicious software, phishing attacks and other modern-day scourges that can invade their privacy, jeopardize the security of their computer and other devices and, in some cases, lead to financial loss, identity theft and damaged reputations. Contrary to what some people might think, children and teens are vulnerable to identity theft[23] because their typically squeaky clean credit histories make them valuable targets. Young people need to understand how to protect themselves from online criminals and hackers not only by knowing how to use protective tools like security software but by understanding "social engineering" – how bad actors can manipulate even savvy Net users into disclosing confidential information. Helping young people learn to protect themselves and their devices from criminals and deceptive social engineering practices can itself be a lesson in media literacy and online safety.

There is also the risk that a young person might do something that gets him or her in trouble with school authorities or the law. Regardless of other consequences, there can be legal or academic sanctions for a wide range of activities, including being depicted online drinking alcohol or illegally using drugs, being involved in gang activity, sexting, cyberbullying, using cell phones to cheat on exams and illegally downloading music and other media.

Further, there is the risk of over-use or obsessive use of technology that interferes with a young person's other activities, including exercise, schoolwork, family time and in-person interaction with peers. Young people need to learn that everything has its time and place and that the inappropriate use of technology (such as texting at the dinner table, or updating their social-networking profile when they should be doing homework, sleeping, or playing outside) needs to be avoided. And adults need to think of how they are modeling this behavior in front of their own children and other youth.

There is the risk of loss of reputation. What we post online can live online forever and what may seem funny or appropriate at the time could turn out to be embarrassing later on. Youth need to understand how to set the privacy features of the services they use and understand that even with these tools in place, it's possible for anything that's posted online (even if they think it's only for their friends) to be copied, stored or forwarded.

Finally, there is the risk of young people being denied access to technology and social media for a host of reasons ranging from financial obstacles, geographic isolation and attitudes and fears that cause adults to deny them access either at home or at school. For some youth, this could be the greatest risk of all because lack of access to technology correlates with lack of access to educational and job opportunities, health care information and participation in modern society.

WHAT WE KNOW ABOUT RISK PREVENTION

It's beyond the scope of this report to go into great detail about all youth risk prevention but there are some things we do know from researchers and risk-prevention practitioners. The first is that a "fear-based approach" is not an effective strategy. Referring to "scare tactics" used in alcohol education projects, sociologist H. Wesley Perkins told the Yale Alumni Magazine that "traditional strategies have not changed behavior one percent."[24]

23 National Crime Prevention Council: "Protecting Teens from Identity Theft" (http://www.ncpc.org/programs/teens-crime-and-the-community/publications-1/preventing-theft/adult_teen%20id%20theft.pdf)

24 Yale Alumni Magazine: "A Closer Look at Alcohol" (http://www.yalealumnimagazine.com/issues/01_05/alcohol.html)

In 1986, Perkins and Alan Berkowitz published a paper which concluded that providing students with evidence that excessive drinking is not a "norm" among their peers had a better outcome than trying to scare them. The norms approach is also a more effective way to curtail bullying. In a paper presented at the 2008 National Conference on the Social Norms Approach, Perkins and David Craig found that "while bullying is substantial, it is not the norm. The most common (and erroneous) perception, however, is that the majority engage in and support such behavior." The researchers found that the "perceptions of bullying behaviors are highly predictive of personal bullying behavior," but that the "norm is not to bully, but only a minority know it."[25]

Based on this research, the commonly repeated mantra that cyberbullying is reaching "epidemic proportions" is counterproductive. Perhaps a better message is to remind youth that most kids don't bully other kids (cyber or otherwise) and that those who do are exhibiting abnormal behavior. Craig and Perkins presented a series of posters used at middle schools with messages like "80% of Crystal Lake 6-8th grade students say students should not treat each other in a mean way, call others hurtful names or spread unkind stories about other students."

The research also shows that most youth are remarkably capable of dealing with Internet problems. A 2008 study on the impact of parenting style and adolescent use of MySpace found that "For all Internet problems, the vast majority of MySpace teens either had appropriate reactions (telling the person to stop, blocking the person from the MySpace page, removing themselves from the situation by logging off, reporting the incident to an adult or to MySpace authorities) or ignored the behavior."[26]

The study also found that "parenting styles were strongly related to adolescent MySpace experiences, behaviors and attitudes." Parents who engage with their children's use of media in an "authoritative" manner (exerting authority while remaining responsive to their children) were more effective than those who were "authoritarian" or "neglectful."

Further, there is some evidence that social networks can be protective in helping to shape and reinforce positive norms. In an online video[27] describing the book *Connected: The Surprising Power of Social Networks and How they Shape Our Lives*, co-author James Fowler observes how social networks (real world or online) can influence behavior. "If your friend's friend becomes obese it increases the likelihood of your becoming obese." But it can also have a positive effect. "If your friend's friend's friend quits smoking then it will also have an impact on whether you're going to quit smoking."

Based on data from the Framingham Heart Study, the two authors found "an individual's chance of becoming obese increased 57% if someone named as a friend became obese in the same time interval," according to an article in the January 23, 2009 edition of *Science*[28].

The same principle can apply to young people online. When he addressed the September, 2009 OSTWG meeting, USC media Professor Henry Jenkins pointed out how young people in online communities tend to have a positive impact on each others' behavior through social norming. "Some of the fan cultures that I've studied," he told the OSTWG meeting, "have incredibly ingrained ethics, ways of teaching, mutual support systems."

25 "Assessing Bullying in New Jersey Secondary Schools" http://www.youthhealthsafety.org/BullyNJweb.pdf

26 "The Association of Parenting Style and Child Age with Parental Limit Setting and Adolescent MySpace Behavior," by Dr. Larry Rosen, in *Journal of Applied Juvenile Psychology*, November-December 2008

27 *Connected: The Surprising Power of Social Networks and How They Shape Our Lives*, by Drs. Nicholas Christakis and James Fowler, Little, Brown and Company, September 2009 (http://www.connectedthebook.com/)

28 "Friendship as a Health Factor" in Science (http://jhfowler.ucsd.edu/science_friendship_as_a_health_factor.pdf)

Jenkins also talked about work he has done with the MacArthur Foundation that found that "kids who engage in participatory practices online also increase opportunities for civic engagement at about the same rate as being on the school newspaper, being on the debate team – the same sort of activities that have traditionally been enshrined as the birthplace of civic skills."

In a 2009 video[29] for the Carnegie Foundation for the Advancement of Teaching, USC visiting scholar and former Xerox PARC director John Seely Brown said it this way: "We have to get kids to play with knowledge." Kids have to be able to "create, reflect and share," and "in that sharing you start to build a whole new kind of culture because you begin to get a kind of peer-based learning … where the kids can learn from each other as much as from the mentor or the authority figure."

So, based on the research and the opinions of several experts, one of the biggest risks to children may be adults who try to shut down the informal learning involved in their use of Internet technologies at home or school.

PREVENTION NEEDS TO BE TAILORED TO RISK

Different kids are susceptible to different risks and need different approaches to prevention and intervention. In 2009, the Internet Safety Technical Task Force concluded that not all youth are equally at risk. Youth with offline high risk profiles tend to be similarly at risk online.

This point was made very clearly at the September 2009 OSTWG meeting by Dr. Patricia Agatston, a counselor and prevention specialist with the Cobb County (GA) School District's Prevention Intervention Center. She is also a trainer, technical assistant consultant for the Olweus Bullying Prevention Program, and co-author of *Cyber Bullying: Bullying in the Digital Age* and cyberbullying curricula for grades 3-5 and 6-12.

At the OSTWG meeting, Dr. Agatston talked about how the Primary, Secondary and Tertiary models that are used in health-related prevention work need to be applied to youth online risk.

- **Primary** prevention includes the basic skills, knowledge and behavioral information that all online kids need. Because most kids don't take extraordinary risks, primary prevention is what should be used for the vast majority of youth.
- **Secondary** prevention applies to kids who are at somewhat higher risk such as kids who live in gang-infested neighborhoods or who have exhibited some early behaviors that are likely to correlate to risk
- **Tertiary** prevention and intervention is used with what are commonly called "high risk youth" who not only need special messaging but, likely, professional intervention with a psychologist or, in extreme cases, in a hospital setting.

Although this framework has been fully accepted by the Centers for Disease Control and other health agencies for prevention of physical diseases and other risks, such as drug and alcohol abuse, it's rarely applied to Internet safety messages or bullying. But Dr. Agatston assured the Working Group that it can apply to online behaviors. "Some of the things that we look at with primary prevention are: What is it that's going to help kids be in a safe environment and grow up safe and have the skills and education

29 "Tinkering as a Mode of Knowledge Product" a video interview with John Seely Brown (http://vodpod.com/watch/1390547-john-seely-brown-tinkering-as-a-mode-of-knowledge-production?pod=cathyinoz)

It's not the Internet
I just the tool

they need to make healthy choices?" While a lot of primary prevention does occur at school, it also takes place in the community, she told the group. "There are certainly things that are already going on right now where it fits, where we could infuse media literacy, digital citizenship, and online safety in all the appropriate areas in the school and in the classroom because that's where kids spend most of their time, obviously, but primary prevention also takes place in the community."

Also, as we have shown above, it is effective to involve peers, not just adults, in risk prevention and education. Social-norm education and peer-mentoring programs have had proven effectiveness in reducing youth risk. For example, Finland has a 38-year-old "peer-support"[30] program that operates in 90% of its schools. Now including Net-safety lessons, the program involves more than 10,000 middle-school-level "peer students" or mentors working with primary school students. The program – which was featured at the European Commission's 2009 Safer Internet Forum – is designed to "increase social responsibility and secure a safe, enjoyable and supportive school year for all," according to the Mannerheim League for Child Welfare in Finland and speaks to the view of U.S. psychologists and risk-prevention specialists that, where schools are concerned, the most likely solution to cyberbullying is a "whole school" approach.[31]

ONLINE RISK CORRELATES WITH OFFLINE RISK

Dr. Agatston reinforced an important finding by the Berkman Online Safety Technical Task Force, which observed, "Minors who are most at risk in the offline world continue to be most at risk online." The Berkman report cited research that found, "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)."

Many of today's Internet safety messages fail to take into consideration the fact that not all youth are equally at risk. The problem with this one-size approach is that the messages are not getting through to the very youth most in need of intervention. It is analogous to inoculating the entire population for a rare disease that most people are very unlikely to get while at the same time failing to inoculate the population that's most at risk.

HOW YOUTH ARE USING SOCIAL MEDIA

In addition to understanding the risks, it's important to understand how young people use social media and technology. In *Living and Learning with New Media: Summary of Findings from the Digital Youth Project*, researchers summarized the findings of the MacArthur Foundation's five-year, $50 million digital media and learning initiative to "help determine how digital media are changing the way young people learn, play, socialize, and participate in civic life."[32]

The researchers found that, "Most youth use online networks to extend the friendships that they navigate in the familiar contexts of school, religious organizations, sports, and other local activities" and that "a smaller number of youth also use the online world to explore interests and find information that goes beyond what they have access to at school or in their local community." Both these "*friendship-driven*" and "*interest-driven* networks" amount to informal learning environments

30 "Peer Support in Schools" from the Mannerheim League for Child Welfare (http://www.mll.fi/en/peer_support_in_schools/)

31 "Bullies: They can be stopped, but it takes a village," by Yale University Prof. Alan Yazdin and Boston College Prof. Carlo Rotella (http://www.slate.com/id/2223976)

32 "Living and Learning with New Media: Summary of Findings from the Digital Youth Project" (http://digitalyouth.ischool.berkeley.edu/report)

where "youth are picking up basic social and technological skills they need to fully participate in contemporary society." The researchers argue that "erecting barriers to participation deprives teens of access to these forms of learning" and that "youth could benefit from educators being more open to forms of experimentation and social exploration that are generally not characteristic of educational institutions."

The implications of the MacArthur research are profound in that they demonstrate how young people have taken it upon themselves to create their own learning environments that, for the most part, are not supported, endorsed or even acknowledged by the formal learning environment called school.

"Unfortunately, many children are not learning effective digital or media literacy skills at home or at school," FCC Chairman said in his presentation of the "Digital Opportunity: A Broadband Plan for Children and Families." In fact, many parents and teachers tell us that they don't sufficiently understand digital technology, much less know how to teach kids about how use it effectively."

Tech educator and author Will Richardson calls it "the decoupling of education and school."[33] And the MacArthur researchers ask, "What would it mean to really exploit the potential of the learning opportunities available through online resources and networks?"

The question is not rhetorical nor is it unrelated to our topic of youth online safety. Now that so much media has a social or behavioral component, learning constructive behavior is part of learning the effective, enriching use of media. But schools' liability fears and extensive filtering, in some cases, causes educators to abdicate their long-held responsibility of guiding and enriching young people's experience with current media.

New-media literacy and citizenship are not just academically enriching, they are also protective in a social-media environment. A 2007 study in Archives of Pediatrics & Adolescent Medicine found that "youth who engage in online aggressive behavior ... are more than twice as likely to report online interpersonal victimization" (Ybarra, et al[34]). Unless new media are used in schools and within families, youth are on their own in figuring out the ethics, social norms, and civil behaviors that enable good citizenship in the online part of their media use and lives. We are not suggesting that schools allow kids to update social network profiles in class but rather that schools find ways to incorporate educational social-technology tools in the classroom to enhance learning and provide pre-K-12 educators with an opportunity to, in the process of teaching regular subjects, teach the constructive, mindful use of social media enabled by digital citizenship and new-media-literacy training – using the media and technologies familiar and compelling to students.

By way of an analogy, imagine if there were no organized sports programs in schools or communities. Kids would still play "ball" in the streets, their backyards and in parks but they would have no formal training in rules, the ethics of fair play or appropriate ways to interact with teammates and opponents. Kids would make up the rules as they go along and would be deprived of all they learn now from coaches, PE teachers and other adults who mentor young athletes. In many ways, that's exactly what is happening with teens' use of social media. They're playing, but there are very few coaches to help them avoid unsportsmanlike conduct and learn to slide home without skinning their knees.

33 "The Decoupling of Education and School: Where do We Begin? (http://weblogg-ed.com/2010/my-educon-conversation/)

34 "Online Behavior of youth who engage in self-harm provides clues for preventive intervention" (http://www.unh.edu/ccrc/pdf/CV160.pdf)

HHS was more fear-based
Not really teaching issue

they happen and the ease with which things happen." NCSA's research backs this up, as 76% of teachers surveyed reported less than 6 hours of professional development on cyberethics, cybersafety, and cybersecurity

An Internet search for "bypass school Internet filters" returns thousands of results. While there are some filtering companies which claim that their software is more kid-proof than others, the bottom line is that a lot of young people know workarounds to filters. Schools could invest more precious resources on tighter filters in a never-ending battle to outsmart their own students, but is that really the way schools should be spending their resources?

The solution, in part, said Donlin, is professional development. "If we have the mandates to teach, to educate minors about online safety, online behavior, it doesn't just happen. We have to take the time to train the teachers, to train the educators and the administrators and the counselors and the professionals who are going to be working with the kids."

And it takes a concerted effort. "Everybody has to be involved. Administrators have to know what they're doing, what they're seeing, how to deal with things. Counselors have to know how to counsel kids, especially the kids who are ... at higher risk because of being harassed or because of things happening to them. We have to include law enforcement. We have to include the industry, we have to include parents, and we have to include the kids themselves," he said.

In a follow-up email, Donlin pointed out that "Much of the [Internet safety] conversation is being led by non-educators, people outside the K-12 world. Others are making 'decisions' which we will have to implement. Not all those decisions – or materials – are educationally appropriate.... K-12 has to be at the table from the get-go. We cannot be handed 'stuff' and told to teach the kids, as we are now mandated to do."

School-based Net-safety curricula

There are numerous Internet safety curricula being used in school districts around the United States and more on the way. Some come from non-profit organizations, some from businesses and publishers and others have been developed by school districts and even individual teachers.

Although individual programs have been evaluated by developers, users and, in some cases, funders, there has yet to be a large-scale national study to look at the accuracy and effectiveness of these programs. And the lack of a coherent evaluation causes David Finkelhor, director of the Crimes Against Children Research Center, to question whether it makes sense for us "to be going to scale with education programs unless they have been evaluated and found to be successful." In an interview for this report, Dr. Finkelhor, who has spent years researching youth risk, said that current programs are typically "based on hunches that people have about messages that young people should be getting." He also questioned whether kids are changing their behavior based on those messages. Finkelhor added that it's important to understand "what the dangers are, who the at-risk individuals are, what the dynamics of dangers are and also what kinds of messages actually prevent those kinds of situations."

Finkelhor questions "whether it makes sense to do cybersafety education independent of a more comprehensive safety and socio-emotional development program." The "skills that we're talking about and trying to develop in terms of making judgments about dangerous situations, not being

mean towards other people, reporting things to or discussing things with adults and parents, taking responsibility for your own behavior and things like that ... these apply in all areas."

Finkelhor joins other youth-risk experts in saying that "fear-based instruction isn't all that effective, that kids need opportunities to role-play situations in order to adapt, to develop new skills. We've learned something about motivation, that they need to sort of feel they have some kind of a stake in it."

Finkelhor also agrees that we need to rethink the "one-size-fits-all" approach to online-safety education but admits that that approach is "less expensive and is also less stigmatizing." He added: "We understand conceptually that kids who are at high risk may need additional or supplementary or different kinds of interventions. In some cases it may be at the level of needing some kind of real psychotherapy to deal with problems that are behind their maladaptive behavior, so if they have anxiety or depression or some underlying mental health issues." Again, he's referring to real-world risk as much as online risk.

The relative lack of information on which strategies are actually effective in increasing youth online safety and responsibility has prompted the National Institute of Justice to fund the CACRC to conduct a study on the effectiveness of youth Internet safety programs. The project, which will likely complete its work around December 2011, will rate and compare the content of four prominent youth Internet safety curricula (Netsmartz, i-SAFE, Web Wise Kids, and the Internet Keep Safe Coalition). The CACRC will also "conduct a process evaluation that will document and evaluate the procedures, audiences and contexts of Internet-safety education programs delivered by ICAC Task Forces and "provide recommendations and piloted materials to ICAC Task Forces to enhance prevention efforts and facilitate future outcome evaluation research."

The project will develop an evaluation toolkit with piloted outcome measures for use in future program monitoring and outcome evaluation efforts as well as an Internet Safety Prevention Clearinghouse or "portal for the placement of Internet prevention education materials and relevant research data."

THE NEED FOR EVALUATION OF INTERNET-SAFETY PROGRAMS

When looking at the effectiveness of any training or curriculum, it's important to consider both whether it is effective in teaching what it aims to teach and whether what it is trying to teach is relevant, accurate and helpful.

For example, much of our Internet-safety education has been focused on helping kids protect themselves from Internet predators, yet, as indicated above, the research shows that the overwhelming majority of students are very unlikely to be harmed by adults they first encounter online. Some will argue that that fact doesn't matter because it's "better to be safe than sorry" but, again, there is reason to question that assumption, based on what we know about the overall lack of effectiveness of "scare tactics," especially when what adults are saying doesn't resonate with young people's own experiences. There is also the risk of youth being "turned off" to authorities if they hear messages they believe to be incorrect. Other risks of scare tactics include focusing on the wrong messages to the detriment of more likely risks and, finally, the risk that fear, rather than motivating, can actually inhibit action.

For example, a 2005 George Washington University study[38] to evaluate the effectiveness of an Internet safety education program found that prior to receiving the training, 25% of the students were unsure

38 "Evaluation of the Effectiveness of the NetSmartz Program: A Study of Maine Public Schools" (http://www.netsmartz.org/pdf/gw_evaluation.pdf

or believed it was safe to post their picture on the Internet but after the training, 96% felt it was unsafe. The same study found that 20% of kids thought it was safe to reveal their real name online but after the training 98% felt that disclosing their real name on the Internet was dangerous.

Clearly that training was effective in changing student's understanding of risk but the larger question is whether that "knowledge" was based on actual risk. When this training was conducted, there was widespread belief among Internet safety advocates and educators that the posting of pictures and personal information was dangerous, but a study conducted by the Crimes Against Children Research Center and summarized in the February 2007 *Archives of Pediatrics & Adolescent Medicine*[39] shows that these particular behaviors don't necessarily correlate to an increase in victimization, whereas "engaging in a pattern of different kinds of online risky behaviors" such as "talking about sex online with unknown people" does correlate with increased risk."

Another set of issues is whether the training is effective and how "effectiveness" Is defined. For example, a 2006 independent evaluation[40] of another training program found that students who had been through the program had "positive and significant" improvement in knowledge, indicating that the program had been effective in getting children to learn about what the program considered to be risky behaviors. However, the study also found that the program didn't significantly change students' behavior. One reason for that was that, even before the program, the majority of students were already using the Internet safely. The "low levels of risky behavior measured at baseline" prompted the researchers to suggest that programs like these "be targeted at youth who have been identified as at-risk for inappropriate behavior or who have been caught engaging in high-risk behavior," adding that "this recommendation does not suggest, however, that the program be taught only to high-risk youth."

The issue of cause and effect also comes up in policy recommendations. For years a number of state attorneys general called upon social network sites to use technology to verify the age of their users, yet a thorough evaluation of the necessity and effectiveness of this technology by the Berkman Center's ISTTF found that age verification is not only not effective but not necessarily advisable. There was some evidence presented to the Task Force that it might actually endanger youth by keeping adult guidance or supervision out of online spaces where peer-on-peer harassment or cyberbullying could occur.

Internet-safety education from the Federal Government

There have been a number of federal resources aimed at Internet safety education going back at least to the mid-90s. Several agencies, including the Justice Department, Federal Trade Commission, the Department of Education, the Department of Homeland Security, FBI and others have, over the years, provided a variety of educational resources online, in printed form, on the Web, and through in-person presentations. In 1997, for example, the Department of Education created the Parents Guide to the Internet,[41] which included a section on "Tips for Safe Traveling" on what the guide referred to at the time as "the Information Superhighway." In April 2000, the Federal Trade Commission launched a "KidzPrivacy" Web site tied to the start of COPPA enforcement. The FBI posted its own "A Parent's Guide to Internet Safety" that warned parents about the dangers of predators and in 2008, the Department of Justice's Project Safe Child launched a public awareness campaign that featured public service

39 "Internet Prevention Messages: Targeting the Right Online Behaviors" in Archives of Pediatrics and Adolescent Medicine, February 2007 (http://archpedi.ama-assn.org/cgi/content/full/161/2/138)

40 *I-Safe Evaluation*, Susan Chibnall, Madeleine Wallace, Christine Leicht, Lisa Lungihofer, April 2006, ICF Consulting Company (http://go2.wordpress.com/?id=725X1342&site=csriu.wordpress.com&url=http%3A%2F%2Fwww.ncjrs.gov%2Fpdffiles1%2Fnij%2Fgrants%2F213715.pdf)

41 US Department of Education: *Parents Guide to the Internet* (http://www2.ed.gov/pubs/parents/internet/index.html)

announcements aimed at children, parents and "potential predators." These PSAs were part of a $2.5 million allocation to fund a national public education and awareness program through partners including the Self Reliance Foundation, Hispanic Communications Network, INOBTR (I Know Better) and the Internet Keep Safe Coalition (iKeepSafe).[42]

Another major federal effort has been the work of Internet Crimes Against Children Task Forces (ICAC). Although their role is primarily in the area of law enforcement, ICAC officers have made themselves available to teach Internet safety to students and parents in communities throughout the country. The 61 ICAC's Task Forces are operated out of local, state and regional law enforcement agencies with support from the Department of Justice.

An ICAC's name says a lot about its mission. It focuses on crimes against children. ICAC officers are well versed on issues such as online enticement and child pornography and not necessarily equipped to handle other areas of youth risk, although some ICAC officers do talk about cyberbullying and other youth-on-youth risks and self-destructive behavior. Still, the emphasis tends to be on the legal and criminal risks which, the expertise of the presenters, and – while an entirely appropriate focus for law enforcement, these are not the risks that research shows students most commonly face online.

Although the Justice Department, with its focus on law enforcement, is probably the most active participant in Internet safety, there are other federal agencies that provide research and educational materials.

The Centers for Disease Control, for example, in 2008 published *Electronic Media and Youth Violence: A CDC Issue Brief for Educators and Caregivers,*[43] focusing on cyberbullying.

The Substance Abuse and Mental Health Services Administration hosted a summit on suicide prevention in 2009 with NGOs in the risk-prevention and Internet-safety fields and presented a white paper on expanding prevention, intervention and postvention (i.e., bereavement support for friends, family and classmates following a suicide) through social media as an effective means for reaching out to and educating youth in crisis. That work continues with the launch in March of ReachOut.com for teens, supported by a nationwide public-service media campaign, "We Can Help Us," all produced in cooperation with the Inspire USA Foundation and the Ad Council. We recognize this important work in this report, not only because SAMHSA will use the Internet to deliver its materials but because issues of youth suicide, eating disorders and self-harm are now impossible to separate from use of the Internet. The Internet can be used to encourage self-destructive behavior but it can also be used to flag, intervene in and prevent such behavior. Young people are alive today because a "friend" (or perhaps a "stranger") recognized their distress signs online and did something to help.

One of the more innovative Federal approaches to Internet safety comes from a coalition of agencies under the umbrella of OnGuardOnline.gov. Operated by the Federal Trade Commission, the project enjoys "significant contributions" from a wide range of partners including the Department of Justice, Department of Homeland Security, Internal Revenue Service, United States Postal Service, Department of Commerce, Securities and Exchange Commission, Naval Criminal Investigative Service, U.S. Army Criminal Investigation Commend, Federal Deposit Insurance Corporation, Commodity Futures Trading Commission, Federal Communications Commission, U.S. Department of Education and several non-profit organizations.

42 Project Safe Childhood National Public Awareness Campaign (http://www.projectsafechildhood.gov/)

43 *Electronic Media and Youth Violence: A CDC Issue Brief for Educators and Caregivers* (http://www.cdc.gov/ncipc/dvp/YVP/electronic_aggression.htm)

One of OnGuardOnline's most successful projects is the publication of *Net Cetera: Chatting With Kids About Being Online*,[44] a 54 page booklet that the agency provides free of charge. The Net Cetera project was mandated by the Broadband Data Improvement Act of 2008 which directed the FTC to "carry out a nationwide program to increase public awareness and provide education regarding strategies to promote the safe use of the Internet by children."

As of the end of May 2010, more than 3 million copies had been distributed through schools, police and sheriff's departments, and PTAs around the United States. The booklet deals with issues including social networking, cyberbullying, mobile phone safety, and protecting computers from malicious software. It's clearly written, based on facts and offers parents and other caregivers easy to understand messages to pass on to children and teens. The booklet emphasizes open lines of communication between parents and kids and advises parents to "be up front about your values and how they apply in an online context."

The Federal Communications Commission is also urging bold moves in the area of technology education. In his March 2010 speech outlining the "broadband plan for children and families," FCC chairman Julius Genachowski spoke of the "four pillars" of his plan: digital access, digital literacy, digital citizenship and digital safety. He called for "teaching kids to think analytically, critically and creatively" and pointed out that "digital citizenship means the values, ethics, and social norms that allow virtual communities, including social networks, to function smoothly. It means having norms of behavior that facilitate constructive interaction and promote trust." Included in the Chairman's definition of safety is, of course, freedom from cyberbullying and harassment but also helping kids deal with harmful websites such as those that promote eating disorders such as anorexia. The chairman highlighted distracted driving as a major concern regarding the safe use of technology.

In the National Education Technology Plan 2010 ("NET plan")[45] that it released in March 2010, the Department of Education called for significant educational reforms that could have a profound impact on Internet safety at school and at home. In what amounts to an endorsement of the use of Web 2.0 technology in schools, the department wants schools to include "the technology that professionals in various disciplines use," including "tools such as wikis, blogs, and digital content for the research, collaboration, and communication demanded in their jobs."

The document points out that "many students' lives today are filled with technology that gives them mobile access to information and resources 24/7, enables them to create multimedia content and share it with the world, and allows them to participate in online social networks where people from all over the world share ideas, collaborate, and learn new things. Outside school, students are free to pursue their passions in their own way and at their own pace. The opportunities are limitless, borderless, and instantaneous. The challenge for our education system is to leverage the learning sciences and modern technology to create engaging, relevant, and personalized learning experiences for all learners that mirror students' daily lives and the reality of their futures. In contrast to traditional classroom instruction, this requires that we put students at the center and empower them to take control of their own learning by providing flexibility on several dimensions."

In a section of the report entitled "Balancing Connectivity and Student Safety on the Internet," the plan addresses the question of whether filters, as required for schools that receive federal E-rate are helping or interfering. "Ensuring student safety on the Internet is a critical concern, but many filters designed

44 Net Cetera: Chatting With Kids About Being Online (http://www.onguardonline.gov/topics/net-cetera.aspx)

45 National Education Technology Plan 2010, US Department of Education (http://www.ed.gov/technology/netp-2010)

to protect students also block access to legitimate learning content and tools such as blogs, wikis, and social networks that have the potential to support student learning and engagement," it points out.

Neither this Working Group nor the Department of Education are necessarily opposed to the use of filters in school, but it is important to recognize that they may come at a "cost," if used in such a way as to block students from social media that could enhance their long-term online safety as well as education.

The NET plan recognizes the reality of how young people use social media and, rather than trying to suppress their use, incorporates those technologies into the learning environment, which can actually be protective. As we pointed out earlier, rather than increasing danger, it can be used to teach students to use these technologies, under the supervision of educators, in a safe and productive manner.

International efforts

While this Working Group is charged with focusing on efforts in the United States, it is important to put our work concerning a global medium into an international context. Just as the Internet makes possible innovative projects like the Flat Classroom Project, an international program that enables middle and high school students to reach across borders to work collaboratively with peers around the world, it also makes it possible for criminals from abroad to reach into American homes and schools. Whether it's the "Nigerian email scam," Trojan horse code written in Russia, or a foreign national trolling the Net to engage in sexual banter with American teenagers, the borders that separate our country from the rest of the world are extremely porous when it comes to the Internet.

Fortunately, there is some excellent work being done around the world ranging from the ground-breaking *Byron Review*[46] in the United Kingdom, which called for "a shared culture of responsibility with families, industry, government and others in the public," to work being done by the European Commission's Safer Internet Program. There is excellent work being done in New Zealand, Japan, Egypt and indeed every other corner of the world and it's important for U.S. educators, safety experts and policy makers to be in touch with their counterparts from other countries.

The Family Online Safety Institute's UK office is in the process of putting together an extensive international compendium of information about Internet safety which will be accessible at www.fosigrid.org when it becomes publically available. The aim of the Global Resource and Information Directory (GRID) is to bring together information, initiatives and best practices from every country into one easily accessible Web site.

RECOMMENDATIONS

The most important recommendation we can make is for all involved with Internet safety education to base their messages on accurate, up-to-date information. Of course, in a changing technology landscape, that's easier said than done, but we can do better.

KEEP UP WITH RESEARCH AND BASE EDUCATION ON IT

There needs to be a centralized clearinghouse at the federal level that disseminates the latest research to all concerned parties including federal, state and local agencies, school districts, professionals who

46 U.K. Byron Review: Children and New Technology (http://www.dcsf.gov.uk/byronreview/)

work with youth and the public at large. This clearinghouse should maintain a website with links to all relevant research material along with summaries written in easy to understand language. It should be updated as relevant research is published. This does not have to be a large or expensive operation as long as it is staffed by people who understand how to locate, summarize, and link to research from a variety of fields including social science, health, youth risk, risk prevention, social media, education technology, and law enforcement along with the latest technology advancements. In addition to summarizing relevant research as it becomes available, this office would also keep stakeholders up-to-date with technology advances that could have an impact on youth and youth safety.

COORDINATE FEDERAL GOVERNMENT EDUCATIONAL EFFORTS

While we are not calling for an "Internet safety czar," we are calling upon federal agencies and departments to coordinate their activities, both internally and with fellow agencies, to ensure that they are basing them on the same accurate research. There needs to be ongoing communications and interaction among all departments involved in Internet safety and education including Education, Justice, Homeland Security, Substance Abuse and Mental Health Services Administration (SAMHSA), Centers for Disease Control, Commerce, the FCC the FTC and the White House with liaisons to Congress and state and local agencies. Federal agencies along with, state and local authorities, members of law enforcement, industry and non-profit organizations need to work together as some have started to do with the FTC's OnGuardOnline. President Obama, in his Cyberspace Policy Review released on May 29, 2009, recommended that the United States initiate a K-12 cybersecurity education program for digital safety, ethics, and security and develop a public awareness campaign. As of this report's date of publication, intergovernmental coordination on these efforts was just getting underway.[47]

TARGET MESSAGING AND TREATMENT

It is very important that messages not only reflect actual risk (as identified in the research) but are also targeted appropriately. We need to focus prevention and intervention where they're needed. Having said that, we cannot ignore high-risk behavior on the part of a small minority, such as inappropriate in-person contact with an adult a minor has met online. That is why we are recommending that Internet education adopt the disease-prevention – and now risk-prevention – model of Primary, Secondary and Tertiary prevention and treatment for youth. Primary is prevention for all children, Secondary prevention targeted at specific risky behaviors and intervention at "teachable moments," and Tertiary prevention and intervention for youth with established patterns of risk behaviors.

PROMOTE DIGITAL CITIZENSHIP AS A NATIONAL PRIORITY

We need to recognize that, by far, the most common risk to children stems from their own actions and those of their peers and that many of these risks are not new. It is the delivery mechanisms which are. While technology can be used to amplify or facilitate bullying, for example, it is not the cause of the problem. In addition to sending a message that bullying and harassment will not be tolerated, work needs to be done starting in Kindergarten or earlier on "digital citizenship" – or rather a renewed effort to teach citizenship online and offline – encouraging children to respect themselves and others. This baseline (or "Primary") online-safety education cannot take place in a vacuum – or only in a single sphere of youth activity – but must promote movement toward greater civility not just among young people but also parents, educators, youth workers and other role models such as media personalities,

47 "Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure" (http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf)

public officials and candidates for office. The government can't legislate civility, but it can encourage it. This will not be an easy fix but, like cutting down on smoking, racism, sexism and other social ills, it can be accomplished through awareness-raising over time.

PROMOTE MEDIA LITERACY AND COMPUTER SECURITY AS A NATIONAL PRIORITY

Children should be taught media literacy, another Primary, baseline, online-safety skill, as soon as they first pick up digital media devices. Knowing how to understand words on a piece of paper, a web page or a TV broadcast is just the start. Children need to understand how to interpret what they read, see, and hear and learn to distinguish between fact, opinion and fiction. And in a social-media environment, media literacy has a new essential component: critical thinking about what is posted, shared, produced and uploaded as well as content that's consumed. Lessons on computer and device security can be taught in the context of learning the same critical thinking taught in media-literacy lessons. Students must be taught not only competency, privacy, and security in the use of technology tools but also the critical thinking skills that protect them from the social engineering behind false advertising and phishing scams.

While tools ranging from content filters to anti-malware programs have their place, they are not a substitute for the lifelong protection provided by critical thinking. The best "filter" is not the one that runs on a device but the "software" that runs in our heads.

CREATE A DIGITAL LITERACY CORPS FOR SCHOOLS AND COMMUNITIES

Consider FCC Chairman Julius Genachowski's proposal for a "Digital Literacy Corps" to "mobilize thousands of technically-trained youths and adults to train non-adopters." In addition to the Corps's community work, it could place trained, tech-savvy recent college graduates or university-age students into classrooms as digital-literacy and social-media experts who could provide an important first step in raising awareness of these critical topics for school-aged children and teachers alike. Programs such as AmeriCorps provide an interesting model for delivering much-needed services and information at the school and community level and coordinating funding for the volunteers who offer their service. Funding mechanisms such as reduced student loan obligations, stipends and other incentives for university age candidates to participate in this first wave of Internet Literacy and responsible Social Media use should be explored.

INCLUDE EVALUATION AS PART OF ALL FEDERALLY FUNDED ONLINE SAFETY EDUCATION PROJECTS

All federally funded online safety education projects should include an independent evaluation component to measure both what they teach and how effective the teaching has been. Evaluation should include changes in behavior as well as changes in knowledge and attitude.

ESTABLISH INDUSTRY BEST PRACTICES

Industry should be encouraged to maintain and expand best practices in consumer education, abuse reporting, customer service and tools/features for safety, privacy and security. Each company needs

to think through what it can do to protect and educate its customers and explore how it can best meet the needs of the different populations within its customer base, taking into account risk levels and other factors. When it comes to safety, the industry needs to work collaboratively with other companies, non-profits, schools and governments. While companies should not be encouraged to compete based on safety, they should recognize that maintaining a safe and healthy environment with respect for privacy is good for business.

Companies should make it easy for users to report abuse ranging from relatively minor terms of service violations to illegal activities and should have sufficient customer-support resources to quickly address these issues and, when necessary, pass them on to law enforcement or other appropriate agencies.

ENCOURAGE FULL, SAFE USE OF SOCIAL MEDIA IN SCHOOLS

Schools need to use and teach the same technologies students are using at home and between home and school. This means not only teaching the same use of social media on fixed and mobile technology, but using social media – in the form of wikis, video, podcasts, interactive word processing, online discussion, etc. – to teach regular subjects already taught in pre-K-12 classrooms. As a national educational priority, teachers of all subjects need professional development to help them understand how to use these technologies and to encourage their productive and safe use. Schools must also understand how to develop effective risk-management techniques and deploy policies, practices and initiatives that include their students' input.

AVOID SCARE TACTICS IN FAVOR OF THE NORMS APPROACH

While shocking stories can sometimes mobilize people, scare tactics simply do not work when it comes to long-term behavioral changes among youth. Scare tactics should be avoided in favor of educational campaigns that model positive behavior and marginalize improper behavior. This is not only true when it comes to harming others or being harmed by others, but self-harm as well. While this Working Group certainly agrees that it's a mistake for young people to allow themselves to be photographed in ways that might question their judgment, it is important to put even this into some perspective, given the number of youth who have engaged in such behavior relative to the ones who have suffered serious consequences. With all potentially negative behavior, it's important that adults do what they can to discourage it but avoid overreaction and "panic" when it isn't called for.

DEVELOP MORE EFFECTIVE RESOURCES FOR PARENTS

Parents need to be more actively engaged in stewarding young people's adoption of technology and safe practices. They need accurate information about risks, solid implementable ideas for the home, places to go to learn more, and clear information about what to do if a problem arises.

RESPECT YOUNG PEOPLE AND GET THEM INVOLVED

There is a commonly held belief that young people need to be protected from either criminals who are out to get them or from their own lack of judgment. While both can be true, it's also important to pay attention to research that shows that many young people have adopted and continue to adopt effective strategies to deflect dangers from both adult criminals and their misbehaving peers. This is not to suggest that youth don't need adult supervision and support but prevention campaigns need to take into consideration the resources that young people bring to the table, both as participants and as leaders. Young people need to be involved in all aspects of risk prevention.

INTERNET SAFETY EDUCATION SUBCOMMITTEE: ADDENDUM A

ANNOTATED LIST OF INTERNET SAFETY EDUCATION LINKS

This list was developed and maintained by the California Technology Assistance Project[48]*, and any editorial comments contained in the list are those of the project and not the Online Safety & Technology Working Group.*

Adina's Deck [Cyberbully Film Project]	Adina's Deck: Solving Cyberbully Mysteries. Three award-winning 30-minute films, website and parent/teachers guide to educate 9-15 year olds about Cyber Bullying, CyberPredators and Plagiarism. **School assembly details** are also available.	Education, Commercial
AT&T Education Advocates Program	AT&T Education Advocates/Directors are credentialed teachers who provide a variety of workshops to teachers, librarians, technology coordinators, and administrators. AT&T's Education advocate, **Linda Uhrenholt** has teamed with CTAP4 to help create and deliver our cybersafety materials.	Education, Commercial
AT&T Internet Safety Land	Developed by AT&T to teach elementary school children about safety and security while surfing the Web. Answer Internet safety questions to help the superhero capture the Internet villain. Complete all the tasks and kids earn a certificate of award. There is also a printable version of the game.	Commercial

48 The California Technology Assistance Project (CTAP) Region 4 (http://www.ctap4.net/projects/cybersafety/cybersafety-education-links-directory.html)

B4UCopy.org	The B4UCopy educational curriculum program has a goal of raising awareness of copyright laws and reinforcing responsible behavior online. Download the free curriculum for elementary and middle school students [**B4UCopy.org/kids**] or the high school curriculum [**B4UCopy.org/teens**] on copyright laws.	Nonprofit
B4USurf.org	Business Software Alliance (BSA) partnership site with an underlying theme of cyberethics and cybersafety. Includes cybersafety tips, teacher guides, cybersafety/ cyberethics lesson plans, free posters, an **interactive quiz**, and two **online games**. There's also a glossary about cybersafety and tips for parents.	Nonprofit
BeWebAware.ca	Funded by Bell and Microsoft, Be Web Aware is a national public education program on Internet safety with resources in both English and Spanish. Covers safety tips for all age groups, K-12 and a "Know the Risks" section on areas of cybersafety. There are links for reporting problems online. Affiliated with the **Media Awareness Network**.	Nonprofit
Berkman Center for Internet & Society	A research program at Harvard Law School founded to explore cyberspace, share in its study, and help pioneer its development.	Education
BNetSavvy.org	bNetS@vvy is a bimonthly e-newsletter offering parents and teachers tools to help kids, ages 9 -14, stay safer online. Primary focal areas include: social networking, wireless devices, gaming, cyberbullying and privacy. Two past issues were devoted to cyberbullying topics. The site is also translated into **Spanish**.	Nonprofit
Boston Public Schools Cyber Safety Campaign	The Boston Public Schools Internet Safety Website is a student-driven site that contains **downloadable resources** and strategies for **parents, teachers and students**. Check out their student video on **cyberbullying**.	Education
Braincells.net	Set in fictitious "Braincells High," Braincells covers computer and cellphone hacking, bullying, and cyberbullying. It teaches kids safe behavior and how to recognize unsafe behavior.	

BSA CyberTreeHouse	Business Software Alliance flash animation site. Includes videos, games, and other information for kids on how to keep cybersafe.	Commercial
BullyingNoWay.com	Learning environment created by Australia's educational community to address bullying, harassment and violence occur in all schools communities. Includes **anti-cyberbullying movies** created by students.	Education
ByteCrime.org	Industry-sponsored set of tools for keeping safe. Identify and protect yourself against threats like computer viruses, worms, spam, spyware, identity theft and online predators. Excellent **hardware security** and **wireless networking tips** can be found here. Their flash video tutorial on **phishing and spoof sites** is suitable for students. Download McGruff the Crime Dog's colorful kids' booklet, "**Mind What You Do Online.**"	Nonprofit
Cafe Aspira	Organized by ASPIRA of NY, a Latino youth services organization. This site is dedicated to promoting cyber awareness, particularly within the Latino community, and to helping parents protect themselves and their children against cyber predators, bullies and frauds. Information on cyberbullying, cybersafety, cyberfraud and cyberpredators is available in English & **Spanish**.	Government
California Cybersafety.gov	The Department of Consumer Affairs has partnered with the California Coalition for Children's Internet Safety to help parents and community leaders protect our children in the online world.	
CTAP Region IV Cybersafety Project	Serves K-12 public education in California. Provides training materials, free posters and information for classroom teachers, school administrators, board members, law enforcement, safe school planning teams, parents and teens.	Education, Government
Center for Safe & Responsible Internet Use	Nancy Willard's site provides research and outreach for educators, parents, librarians and policy makers. Nancy is author of two books and has published extensively in professional journals. Check here for in-depth coverage of legal issues, presentation notes, reports and links to her publications.	Nonprofit

Chat Danger Online	Learn how to keep safe while chatting online. Practical advice for use of cell phones, chat, email, messenger and games. Includes real-life stories. Site developed by Childnet International.	Nonprofit
Childnet International	UK-based non-profit organization working with others to help make the Internet a great and safe place for children. Includes "Know It All" sections for teachers and parents. Connections are made to the ICT program of study. Many of the award-winning resources are available on a CD/DVD, free to local teachers. See also: **Digizen.org**	Nonprofit
ChildrenOnline.org	Workshops, research and tools for parents and schools with practical real-life solutions to the issues faced by young people online. Site was developed by two credentialed secondary teachers, who are also authors of a new ISTE book, **Safe Practices for Life Online.**	Education
Common Sense Media	Offers educator kits for **teaching digital citizenship**. See: **Internet Survival Guide** for Parents. Their video, **"A Common Sense Guide to Internet Safety,"** would be ideal to present at a PTA Meeting.	Nonprofit
ConnectSafely.org	The ConnectSafely forum is co-directed by cybersafety experts, Larry Magid and Anne Collier. Forum, safety tips in English and Spanish, videos, printable tips.	Nonprofit
Crimes Against Children Research Center	University-based research center. Check here for the real stats, myths vs. realities on child predators. **Internet Safety For Teens: Getting it Right** is a fact sheet, packed with clarifying information for your next presentation.	Education
Cyber Exchange	Download free posters suitable for GR 6-12 classrooms on sexting awareness, firewalls, cyberpredators and cybersecurity from Cyber Exchange, a Cyber Security Awareness program and nonprofit that provides education and certification for information security professionals.	Nonprofit
Cyberbullyhelp.com	**Three school psychologists** (trained in Olweus Bullying Prevention techniques) have applied their knowledge and expertise to cyberbullying in the digital age.	Education

Cyberbully411.org	Cyberbully411 is an effort to provide resources for youth who have questions about or have been targeted by online harassment. The website was created by **Internet Solutions for Kids, Inc** with funding from the Community Technology Foundation of California.	Nonprofit
Cyberbullying Research Center	Two criminal justice specialists provide up-to-date information about the nature, extent, causes, and consequences of cyberbullying among adolescents.	Nonprofit
Cybercitizenship.org	The Cybercitizen Partnership was established by the Information Technology Association of America (ITAA) Foundation and the United States Department of Justice to establish a broad sense of responsibility and community in order to develop in young people smart, ethical and socially conscious behavior.	Nonprofit, Government
Cybercrime.gov	Department of Justice site on Cyberethics for Kids. Provides model acceptable use policies, info about being a good cybercitizen, rules for cyberspace, a **lesson plan outline** and links to other sites.	Government
Cybersavvy.org	A joint effort of the Direct Marketing Ass'n, AARP and **OnGuard Online** to help new and seasoned users protect their privacy and safely explore cyberspace.	Nonprofit
Cybersmart.org	Safety and skills for the 21st century. **Standards-based lesson plans** and activity sheets for K-12 students. The focus is on creative inquiry, fostering collaboration skills and critical thinking.	Education, Nonprofit
Cybersmart Detectives	From Childnet International and the Australian Government, this online game teaches four key internet safety messages and is designed to be played in a school environment. Limited to United Kingdom schools. A **promotional video** explains the project.	Nonprofit, Government
Cybersmart Kids Online	Community awareness project developed by the Australian Communications and Media Authority (ACMA). The site contains cyber rules, chat rules and mobile rules for kids as well as links to safe sites. Australian schools can also register for access to the online game, **Cybersmart Detectives**, in which players learn about managing bullying behaviors both offline and online.	Nonprofit

Digital Citizenship.net	KSU Professor, Mike Ribble's personal site on digital citizenship. The **Nine Elements of Digital Citizenship** should help shape educational efforts behind any cybersafety and cyberethics program.	Education
DigitalCitizenshipEd	Free online curriculum that focuses on creative rights in the world of digital citizenship. Addresses music, video, writing, software and images through thematic curriculum units that are ISTE aligned.	Nonprofit
Digizen.org	Practical advice on cyberbullying, using social networking sites safely and creatively, and being a good net citizen. Check out their **cyberbullying films** and teacher guides. Site is owned by Childnet International.	Nonprofit
Disney Online/Safe Surfing	**Safe Surfing with Doug**: 9 comic book style games and activities that help kids learn appropriate behaviors online (Disney UK Site).	Commercial
Dizzywood	Subscription-based virtual world with some free activities and content for kids. Click on the **video presentation** to learn how sixty GR 4-5 students in Marin County, CA used Dizzywood to learn about core social values and digital citizenship. More info about the school project is provided in this **podcast**, starting at 4:30 minutes into the broadcast.	Commercial
Don't Believe The Type	Missing & Exploited Kids site. Kids learn about the dangers of the internet, online chatrooms, instant messaging, social networking sites, situations to avoid and how to keep their identity private. Three **PSA's** are included. Resources are available in English and Spanish.	
EdZone/K12HSN	The California K-12 High Speed Network (K12HSN) provides this free suite of Web 2.0 tools to enhance today's classroom environment for students in the public school system.	Education, Government
Enough is Enough	Protecting our children online. Site focuses on public education about exposure to pornography and predators online.	Nonprofit

Family Online Safety Institute	International space for open discussion amongst stakeholders, exploring the challenge of how to keep children away from images, words and sites that their parents do not want them to see, and from behaving in ways that expose them to unnecessary dangers, without restricting wider online freedom.	Nonprofit
Family Resources Web Site [Symantec]	Symantec's Family Online Safety Guide won the 2008 iParenting Media Award and is a free download, available in English and Spanish. Register for the free newsletter. You can also find Internet Safety Advocate, **Marian Merritt's advice column** for parents here. Download articles from their **extensive library** or visit **Online Family Norton**, to learn about their product for managing kids' time online.	Commercial
FBI-SOS Internet Challenge	Internet safety program designed to help students recognize potential dangers associated with the internet, email, chat rooms and social networking sites. The program addresses and defines topics serious in nature such as seduction, child pornography, solicitation, exploitation, obscenity and online predators. Students participate in a **scavenger hunt**, take web-based quizzes and review specific web sites aimed at promoting online safety.	Government
GetNetWise.org	Developed by a coalition of Internet industry corporations and public interest organizations. This site provides a database of filtering tools for families: browsers for kids, tools that limit time on the computer, spam filtering tools etc. They have some helpful video tutorials on **using privacy settings with MySpace and Facebook.**	Nonprofit
Hector's World	Web-based animations and interactive educational activities in a rich graphic environment where elementary students learn digital citizenship skills. Take the **teacher site tour** or check out **teacher and parent** information. Each of the Hector's World episodes has accompanying **lesson plans** and storybooks. Part of **NetSafe**, New Zealand.	Nonprofit
Identity Theft Portal	Identity Theft Portal is an online resource for identity theft protection and identity theft victims. Provides information by State.	Nonprofit

IKeepSafe	Internet Safety Coalition with resources for parents and young kids, including **FunZone games**. Be sure to check out the flash tutorials on **Social Networking Basics** and their collection of **PSAs.** IKeepSafe provides digital citizenship training using a **C3 Matrix** of concepts: cybersafety, cyberethics and cybersecurity.	Nonprofit
iLearn Online	Partnership between iSafe and Microsoft to provide an "On Demand" system for Internet safety education. These training modules teach and/or train other educators on the iSAFE curriculum.	Nonprofit/ Commercial
Internet Safety with Professor Garfield	Online series of interactive, animated lessons. Comprised of a narrative tutorial (WATCH), guided practice (TRY), and an interactive challenge (APPLY), each lesson delivers a supportive and scaffolded learning environment for students. This site was developed in partnership with the Virginia Dept of Education.	Education
Internet Solutions for Kids (ISK)	Dr. Ybarra is an expert in the field of Internet victimization, with publications in cyberbullying, sexual solicitation, and related mental health and social characteristics of children. ISK has partnered with Dr. David Finkelhor and his colleagues at the **University of New Hampshire Crimes Against Children Research Center** to examine current issues in cyberbullying, blocking software, and more. ISK also hosts the site, **cyberbully411.org**.	Education
i-Safe, Inc.	i-SAFE offers a prevention-oriented Internet Safety Education program with interactive age-appropriate units of instruction designed for upper elementary, middle, and high school levels. There may be a fee for some materials.	Nonprofit
Join the C-Team	Comprehensive educational program of the Entertainment Software Association that introduces the concept of intellectual property to students in grades K-5 with hands-on activities that enable them to discover the natural connection between copyright and creativity.	Nonprofit

Kids Help Phone	Canadian nonprofit group offering phone and online counseling for kids. Be sure to check out their **PSAs** on bullying and cyberbullying.	Nonprofit
Kidsintheknow.ca	Kids in the Know is an interactive safety education program for increasing the personal safety of children and reducing their risk of sexual exploitation. Download a free copy of their colorful 16-page comic book [**Zoe & Molly Online**] for 4th grade students to address risks associated with children sharing personal information and sending pictures online. There is also a pre- and post-test.	
Kidz Privacy	Materials on this web site are provided by the FTC and are built around support for COPPA, the Children's Online Privacy Protection Act. Resources include basic advice for kids, tips for parents and downloadable teacher guides that include coverage of protecting student identities online.	Government
KinsaNet	The Kids International Safety Alliance (Kinsa) provides training for law enforcement and the general public on child exploitation. They work with well-known kids' properties to educate kids in environments that they know and love. Download their cyber safety comic, **Grossology: Web of Deception**. A **teacher's guide** is also available.	Government
KnowWhereTheyGo.org	Project Safe Childhood national media campaign to combat the increase of sexual predators using the Internet to entice and sexually exploit children. Stresses importance of knowing where your kids go online. Includes **video PSA's**, webisodes, radio PSA's and transcripts available in both English and Spanish. Site offers links to a **digital library** of free multimedia resources available by topic.	
Look Both Ways Foundation	Provides information on internet safety, security, privacy and ethics and a Skills for Life Online curriculum free of charge for K-12 schools.	Nonprofit
Make A Difference for Kids, Inc.	Non-profit organization dedicated to the awareness and prevention of cyberbullying and suicide through education.	Nonprofit

McGruff.org	Internet Safety stories, games, videos and tools for kids and parents from McGruff and the National Crime Prevention Council. Download their poster, **Internet Rules of the Road**.	Nonprofit
Media Awareness Network	The Media Awareness Network has created games and interactive student modules for K-12 students (complete with extensive Teacher's Guides) to help kids to develop cybersafety skills. Site is also accessible in **French.**	Education
Megan Pledge	Named in honor of Megan Meier, who took her own life rather than face continued harassment at the hands of a neighborhood mom posing as a cute 16-year-old boy. The campaign seeks one million teens to take a pledge against cyberbullying in Megan Meier's name.	Nonprofit
Michigan Cyber Safety Initiative (CSI)	Includes templates and handouts for student, teacher and community workshops as well as **videos** from other agencies.	
MindOh!	Download their "Cyberbullying Thinking it Through" worksheets and use them as discussion starters with kids. Students assess their own beliefs and attitudes, consider past experiences, and explore ways of making smarter choices in the future. Cyberbullying Lesson Plans are also available on cyberbullying, predator and privacy topics.	
MySpace Dept. of Safety & Security	Safety videos, MySpace Guides for Parents and School Administrators, **ParentCare Software** downloads, and flash tutorials on **social networking basics**.	Commercial
MySpace MyKids	Interactive video sessions that educate parents on MySpace and equip them to tackle the online issues that teens may face.	
MySpace Pause	A collaboration between Fox Network Group and Kaiser Family Foundation. Stay informed and stay in control. It only takes a minute to change your life. That's one minute to stop, think, pause and consider the consequences of your actions. Site includes PSAs and informational resources.	Commercial Nonprofit

NetAlert Cybersafe Schools	NetAlert is the Australian Government's online safety program. Primary grade students can follow a flash animation adventure called **CyberQuoll** while students in secondary grades have their own hip adventure called **Cybernetrix**. Teacher support materials are also available.	Government
NetBasics.org.NZ	Launched in April 2008, this award-winning site from New Zealand is composed of 10 highly entertaining flash animations following the travails of the Jones family as they negotiate their way around the Internet. The series includes a collection of good and bad characters in fictional adventures that engage users while they deliver a serious message about the security threats we face every day online.	Government
NetFamilyNews	A weekly electronic news service to inform and educate parents, families and caregivers of children who spend time online. Well written, accurate and timely information from Internet Safety expert, Anne Collier.	Nonprofit
NetSafe, NZ	NetSafe provides cybersafety education for all New Zealanders - children, parents, schools, community organisations and businesses. The ISG has been designated the Ministry of Education's 'agent of choice' for cybersafety education in New Zealand.	Nonprofit
Netsmartz.org	Interactive, educational safety resource from the National Center for Missing & Exploited Children® and Boys & Girls Clubs of America for children, aged 5-17, parents, guardians, educators, and law enforcement. Great **"real life stories"/flash videos** and **activity cards** for classroom use and lots of online/ offline activities for younger kids. Activity cards are also available in Spanish.	Nonprofit
Netsmartz Education	Instructional and classroom materials and videos in both English and Spanish, coded for grade-level appropriateness. Train-the-trainer materials are also available. A drop-down menu provides direct links to pages customized for each state, to make it easy to form educational partnerships.	Nonprofit
Netsmartz 411	Internet Safety Help Desk	

Nortel IT	An initiative of Nortel Community Relations to prepare teachers, students, and learners of all ages to develop 21st century skills. Lesson plans, guides, activities, PowerPoint files and videos cover digital citizenship topics like **viruses and spam, digital ethics, predation** and **cyberbullying.** The site is translated into multiple languages, including **Spanish.**	Commercial
Northwest Learning Grid(NWLG)	Educational site from England uses colorful graphics and flash-based quizzes to test student skills in **digital literacy.** Most questions focus on conducting useful searches and finding the best information. Elementary and secondary students can also play five **e-Safety games** to demonstrate knowledge of appropriate online safety behaviors.	Education
NSTeens.org	Part of Sprint's 4NetSafety Program. Content for this site was created by NetSmartz and covers topics like social networking and cyberbullying. The site uses flash-based **comics** and **videos** to explain how to use the Internet safely and avoid cyber-bullies and predators.	Nonprofit
OnGuardOnline	FTC site that provides practical tips from the federal government and the technology industry on topics such as identity theft, spyware. phishing, spam and ecommerce/ shopping online. Their colorful flash-based quiz section would be great for student use and includes **13 games** that help kids test their cybersmarts. Resources are available in English and **Spanish.** Schools can order bulk copies of **NetCetera: Chatting With Kids About Being Online** to send home to parents.	Government
OnlineFamily.Norton	Parental control service that allows parents to manage and monitor their child's time online. Watch this **video** to see how it works. There is a subscription fee involved.	Commercial
Passwords are like underwear... Poster Program	Developed by the IT Dept at University of Michigan, this series of five clever posters gets users to remember and adopt a few basic principles of password security. You can order copies off of their web site.	Education

PBSkids.org: Get Your Web License	If kids answer all 10 questions about surfing the Internet correctly, they may print themselves a web license.	Nonprofit
Play It Cybersafe	Learn about cybercrimes. The Cyber-Crime and Intellectual Property Theft Prevention and Education Project is a United States Department of Justice funded initiative to educate the public on cyber-crime and intellectual property theft.	Government
PointSmartClickSafe.org	The Cable Industry's effort to educate parents about protecting their child's identity online. Click on the video link at the bottom of the page to access six flash videos: Internet Safety Pledge, media literacy, phishing and predators, kids' blogging content, privacy issues, etc. Resources are in English and Spanish.	Commercial
PowerToLearn.com	Interactive case studies exploring 8 topics: Wireless, Social Networking, Digital Permanence, Cyberbullying, Misinformation, Fair Use, Privacy and Downloading. Through multimedia activities, students examine issues affecting school work, class papers, entertainment activities, and online safety. "Power to Learn" is Cablevision's nationally-recognized education initiative. Some resources are available in Spanish.	Commercial
Professor Garfield Foundation: Internet Safety & You	Garfield animated comics educate kids about cyberbullying, online safety. Other topics in development include digital and media literacy. Students watch animated lessons, try interactive, guided practice and apply knowledge to earn safety certificates. Includes downloadable teacher lesson plans. A joint project of the Virginia Dept. of Education and the Professor Garfield Foundation.	Government/ Nonprofit
ProtectKids.com	Practical advice on internet dangers, including pornography and sexual predators from Donna Rice Hughes, author of **Kids Online: Protecting Your Children in Cyberspace.**	
Rochester Regional Cybersafety & Ethics Initiative (RRCSEI.org)	Rochester Institute of Technology-led community effort to improve cyber safety, security and ethics at the K-12 level. Educator partnership with NetSmartz. See also their findings from a 2007-2008 **RIT Survey of Internet and At-Risk Behaviors of 40,000 K-12 students [PDF].**	Education

SafeKids.com **SafeTeens.com**	Safe Kids.com and SafeTeens.com are blogging sites operated by cybersafety expert, **Larry Magid** and in connection with **ConnectSafely.org**. The sites contain information about the dangers of children using the Internet, rules, advice, and tips relating to child security and the web.	Editorial
SafePassageMedia	Bullying prevention program and **award-winning videos**. SafePassage Media was formed in 2007 for the sole purpose of creating and distributing two public awareness DVDs related to the suicide of 13 year old Ryan Halligan, a cyberbullying victim.	Nonprofit
SafeSurf Kids	Florida's Internet Safety site for young kids. Kids can learn about the Internet with games and activities. See also, the SafeSurf companion site for **teens**.	Government
Simple K12 InfoSource	In addition to the online curriculum and training lessons, the program includes assessments, quizzes, and a safety pledge for students, safety plans for teachers, and a self-assessment and resources for parents.	Commercial
Smart AUP	The Smart AUP is a fast, simple, assessment tool designed to allow students to demonstrate their knowledge of the rules and provisions outlined in a standard Acceptable Use Policy (AUP). Developed by **FBI-SOS** for the State of Florida.	Education, Government
Smart Online/Safe Online (SOSO)	Non-profit social initiative that uses kids to deliver campaigns aimed at educating their peers about cyberbullying/cybersafety issues. Check out their **video** on cyberbullying and an online game called **"Web Warriors"** where kids create their own avatars and complete missions that educate them about cyberbullying, social media and mobile safety.	Nonprofit
SocialSafety.org	Started in January 2008 by the founders of MyYearbok.com, SocialSafety.org is an effort to educate U.S. teens on the dangers of social networking. Social Safety provides hundreds of thousands of free safety education packets for U.S. high school students, and provides free safety content to any student or site that requests it.	Nonprofit

StaySafeOnline.org	The National Cyber Security Alliance (NCSA) is a collaborative effort among experts in the security, non-profit, academic and government fields to teach consumers, small businesses and members of the education community about Internet security.	Nonprofit
StopBullyingNow!	U.S. Department of Health and Human Services offers flash movies, games, and information about bullying and how to prevent it. Some of the flash movie **"webisodes"** focus on cyberbullying. Closed captioning and Spanish versions are available.	Government
StopCyberbulling.org	Part of the Wired Safety group's effort. Includes a flash presentation, Parent's Guide to Cyberbullying.	Nonprofit
SurfSwell Island	Adventures in Internet Safety with Mickey and the Gang, delivered in typical Disney style. Features include "smart-surfing" lessons where kids learn about privacy and netiquette through entertaining and interactive activities, educational games, and hands-on experiences.	Commercial
That's Not Cool	Web site developed by the National Teen Dating Abuse Hotline. Great **PSA's** on teen abuse of technology through controlling behaviors like excessive text messaging, pressure for digital photos, stalking, privacy problems and rumors.	Nonprofit
Trend Micro Web Security and Internet Safety	Commercial company with an interest in promoting Internet Safety for kids. Content covers privacy issues, mobile safety, identity theft, cyberbullying and computer security issues. There is also an **Internet Safety Blog** for Parents and Schools.	Commercial
The Children's Partnership	National nonprofit, nonpartisan child advocacy organization - goal is to ensure that **digital opportunities are available to all young people**, especially those that are low-income and underserved. **ContentBank** is one of their affiliated web sites. Great video here, **"Why Does Technology Matter for Youth?"** Agency also has downloadable PPTs and guides for child safety online.	Nonprofit

The Socrates Institute/ CyberEthics Project	An educational program to address the problem of juvenile cybercrime. The K-12 project in CyberEthics is in development and will have classroom, video, and web-based learning materials including videos of actual case studies of juvenile cybercrimes (e.g. hacking, software piracy, illegal downloading, cyberbullying).	Education
Virtual Global Task Force	The Virtual Global Taskforce (VGT) is made up of police forces from around the world working together to fight online child abuse. Check out their PSA, **"Think You Know Who You are Talking To?"**	Government
Web Wise Kids	Community and parental resources for Internet safety. They have developed three interactive cybersafety adventure games (**Missing, Mirror Image** and **AirDogs**) that are excellent for classroom use. WWK was recently awarded funding from Verizon to develop a game to educate students about responsible use of cell phones. **Katie Canton's story** (told on video) is also excellent for student learning.	Nonprofit

INTERNET SAFETY EDUCATION SUBCOMMITTEE: ADDENDUM B

EXAMPLES OF INDUSTRY-PROVIDED NET SAFETY PROGRAMS

AOL

AOL has been a strong advocate of Internet safety since its early days as the nation's largest dial-up online service, when it pioneered the use of parental controls, special kids-only services, and Internet safety information. In 1996, AOL became the sponsor of one of the nation's first Internet safety websites and, despite a rather tumultuous existence since its merger with Time-Warner in 2000 and subsequent separation in 2009, AOL has remained committed to Internet safety.

The company operates a SafetyClicks blog (blog.safetyclicks.com/) featuring industry and advocacy experts who provide parents, teens and kids with information and tools to help keep themselves and their families safer online. The blog covers a wide variety of topics related to child Internet safety, social networking, cyberbullying, sexting, sharing information online, Internet lingo, and more. AOL also operates AOL Internet Security Center where it has educational materials and tools for computer security.

A company official said that AOL works within the educational community to bring Internet safety to the schools by providing online safety education in the form of formal presentations or hands on demonstrations at schools, for PTA meetings, and other organized meetings. AOL also supported the Virginia Internet Safety Curricula requiring state schools to provide an online safety course and, internationally, AOL worked with teachers and education authorities to develop Internet safety materials and lesson plans specifically for teachers. AOL provides context-specific safety messages in areas where young people and others make decisions about how to interact with the community.

The company provides support to nearly a dozen national-level Internet safety organizations offering a variety of programs and materials to schools and families.

AT&T

AT&T's "Stay Connected, Stay Safe site" (att.com/safety) offers safety tips and interactive safety games for both its wireline and wireless services. Its "Wireless Smart" section, for example, includes "a parents' guide to texting" and information about its "Smart Limits" program that enables parents to put controls on their children's phones. There is also extensive Internet safety information including access to PDF files of some of the company's printed brochures for distribution offline.

AT&T has taken the initiative to combat the dangerous practice of texting while driving with a campaign called "It Can Wait." The new national campaign, according to a company press release, "features true stories and the text message that was sent or received before someone's life was altered, or even ended, because of texting and driving." FCC Chairman Julius Genachowski mentioned distracted driving in his "broadband for kids" speech: "A quarter of U.S. teens with cell phones say they have texted while driving," he said, adding that "according to the National Highway Transportation Safety Board, 80% of fatal teen accidents are caused by distracted driving."

The company also took its safety show on the road through the AT&T Hometown Tour, which, according to AT&T "visited more than 100 communities nationwide and worked with more than 20,000 students from Connecticut to California on Internet safety lessons, programs, and workshops geared toward elementary and middle-school-aged students." AT&T also supports the consumer-safety education programs of a number of national Net-safety advocacy organizations.

Comcast

In October 2009, Comcast unveiled its Constant Guard Internet Security Program, designed to protect its broadband customers from bots, viruses, and other online threats. The program provides protection to children, whose email accounts can be spammed by bots with links to objectionable content.

As a part of its partnership with Symantec, Comcast HSI customers have access to OnlineFamily.Norton at no additional charge. OnlineFamily.Norton gives parents the ability to monitor where children go, how long they are online, who they talk to, and what information they are sharing with others.

Comcast and Kidzui have a partnership to deliver a safe, fun Internet portal for kids and families to millions of households across the country. Designed for children aged 3-12, KidZui connects kids to games, activities, videos, and educational materials – all of which has been reviewed by an editorial team of parents and teachers.

As part of National Internet Safety Month in June 2009, Comcast and McAfee partnered to call on parents and their children to take the *Cyber Summer Safety Challenge*, designed to start a dialogue about Internet safety and online threats, and what children and teens can do to protect themselves.

The Challenge included both a kid's version and a teen version of online safety issues for parents and their children to talk through. Comcast also works with Internet safety organizations such as FOSI and iKeepSafe.

In its partnership with iKeepSafe, Comcast rolled out state-specific Internet safety "Parent Presentations" in several states, including Florida, Maryland, Michigan, Mississippi, New Hampshire, Texas, Virginia, and Washington, in 2008 and 2009, in coordination with each state's Attorney General. Comcast has coordinated efforts to distribute these Parent Presentations throughout the schools in these states and continues to host these Presentations On Demand for its video customers. Comcast has also sponsored and helped distribute Faux Paw and the Dangerous Download in the Faux Paw series, a book and DVD series that educates children about the dangers and potential pitfalls online.

Comcast provides Comcast SafeSearch, a kid-safe Internet search tool, powered by Google. Comcast also offers an email feature that enables parents to limit who their children may receive email from (e.g., parents can create a specific list of individuals who are allowed to send email to their children, thus blocking email from spammers advertising material parents may find objectionable).

Finally, Comcast implemented controls that allow authenticated customers using the new Fancast Xfinity TV service to set up account "families" consisting of primary and secondary account holders. Primary account holders can restrict secondary account holders' access to Fancast Xfinity TV content, either by network or by rating. Users within a particular family account have to enter a four-digit PIN prior to viewing a video that has been restricted on that account. In connection with these controls, Comcast uses an opt-in feature contemplated by the Children's Online Privacy Protection Act (COPPA), which prompts a primary account holder, during the online parental control set-up, to read and complete a COPPA disclosure and a COPPA consent screen. For each restricted secondary account, a primary account holder must affirmatively consent to the collection and use of personal information for children under 13 years of age.

Facebook

Facebook has a privacy link at the bottom of each page and, as of this writing, was in the process of building out a Safety Center with help from its Safety Advisory Board. The growing safety board currently consists of representatives of six national and international non-profit organizations. Facebook also provides funding to support these organizations' own consumer-education programs.

In December 2009, Facebook announced new privacy settings and took the unprecedented step of requiring all of its members to configure their privacy settings. Although there was some pushback about the company's default settings, the exercise forced more than 300 million people around the world to put at least some thought into privacy.

In addition to its safety education pages, the company builds "contextual messaging" into the product. For example, when news users go through the registration process they are introduced to some basic concepts, but as they start posting information on the service they are reminded about privacy options. For example, when someone updates his status, there is a little lock icon that shows the current privacy settings for that piece of content and allows the user to change those settings.

As part of a court settlement, Facebook has agreed to allocate $6 million to an independent foundation that will fund research- and advocacy-related programs in the areas of user privacy and safety. In addition to the non-profits it supports, Facebook also supports the national Crimes Against Children Conference presented annually by the Dallas Children's Advocacy Center and the Dallas Police Department.

Microsoft

Microsoft focuses on three areas to make computing and the Internet safer for children. These three areas are 1) tools and technology, 2) guidance and education and 3) law enforcement and public policy.

Microsoft builds free family and safety tools and parental controls into a range of products and services, including Windows operating system; Windows Live online services; the Xbox 360gaming platform and Xbox LIVE online gaming environment; the Zune digital media player; and the Mediaroom digital video platform. These tools let parents decide when children can use the computer, which Web sites they can visit, which software applications they can use, which games they can play and with whom they can interact online. In addition, Microsoft provides Windows users a free anti-virus and anti-malware program.

Microsoft's online safety and privacy center (www.microsoft.com/protect) provides safety, privacy and security guidance. This site includes brochures and videos covering topics from safer online gaming and social networking to building stronger passwords and avoiding cyberbullying.

In 2009, Microsoft launched a public service initiative called Get Game Smart (www.getgamesmart.com) with more than a dozen children's media advocacy groups. The Get Game Smart campaign is dedicated to educating families about safer and more balanced digital media consumption.

Microsoft partners with government agencies and NGOs to encourage comprehensive public education on safer, more responsible behavior online. In addition, Microsoft helped develop the Federal Trade Commission's online safety Web site, OnGuardOnline.gov.

MySpace

MySpace has a "Safety tips" link at the bottom of every page which includes links to safety videos, tips and settings, and resources from a variety of national and international non-profit groups. The company, according to officials, offers educational materials targeted to different constituents, including law enforcement, schools and parents. Resources include a guide called *MySpace Safety for Parents and Educators*. MySpace and News Corporation Chief Security Officer Hemanshu Nigam (who is co-chair of this Working Group) has his own MySpace page, where he blogs about online safety and security, especially as it applies to MySpace. He also speaks frequently at law-enforcement conferences.

The company created a guide specifically for law enforcement and has trained more than 4,000 police officers in person. A guide has been distributed to more than 100,000 school officials. MySpace provides dedicated toll-free numbers to connect law enforcement and school personnel to its customer-service department when user behavior becomes harmful.

MySpace is currently or has previously partnered with a number of non-profit agencies, organizations, and associations and works with the Internet Crimes Against Children Task Forces (ICAC) nationwide.

In its site, MySpace offers contextual training in addition to the centralized safety learning tools it provides. For example, as a user clicks on a link that takes him off the site, he is warned that he's going

to a page not vetted by MySpace. There are even more strenuous warnings if a user is about to go to a page believed to contain malicious software, according to a company official.

Ning

Ning is a unique, rapidly growing social network service that currently hosts some 2.3 million user-created, interest-based or "vertical" social network sites that together serve about 45 million people. Ning gives moderators, the people who set up their own networks, control over who can access them and how they're used and policed.

Ning has a safety center that provides general safety tips and a set of tips aimed at teens and another for parents. There is also instruction to help members use the services privacy and safety controls. Ning also engages its members to provide input on what is and isn't working when it comes to safety and privacy tools.

The service has a robust Help Center that offers tutorials to help moderators set up and manage their sites' privacy and safety tools. Because the network moderator or community leader has so much control, the service has been attractive to teachers, many of whom have set up networks for the exclusive use of their students or perhaps their students and parents. Teachers who are using Ning (or other services) in the classroom afford students opportunities to learn safety, privacy and citizenship in the context of the subjects being taught with Ning.

Ning provides support for several Net-safety nonprofit organizations and works closely with the National Center for Missing & Exploited Children, according to a company official. The company also participates in a Cyber Hate Strategy Group organized by the Stanford Center for Internet and Society and the Anti-Defamation League. This group consists of members in industry, academia and NGO's and will examine approaches of tackling the problem of cyber hate.

Verizon

Verizon's Parental Control Center (http://parentalcontrolcenter.com/) not only provides access to how-to information about the company's parental control tools but also to advice about mobile and online safety. This includes links to resources from NetSmartz and other programs educating youth and parents on a variety of safety topics. The Verizon Foundation's ThinkFinity.org site provides materials for teachers and parents on identity protection, Internet and mobile safety and related topics. Verizon and its foundation provide support for a variety of safety projects including conferences and the recently aired PBS Frontline program *Digital Nation*.

Yahoo

Yahoo operates a safety site (safety.yahoo.com) that has separate areas for teens and parents. The teen section has resources and links to teen-centered safety programs including iMENTORs and WiredSafety's TeenAngels. The parents section and the main page have links to Internet safety bloggers from a number of national Internet-safety organizations. The site also hosts comprehensive guides for safer practices in using its mail, online groups and mobile service. There is also safety information in the parents sections of Yahoo Kids and Yahoo Shine, with links to safety articles written by Yahoo staff and safety experts from non-profit organizations. There are also sections with "tools and tips" that deal with a variety of safety-related subjects

The company works with law enforcement to educate middle school students on safer practices by offering annual assemblies and has helped law enforcement create an original "restorative justice" diversion course for youth who have mistakenly engaged in risky online behaviors.

Yahoo also organizes and hosts an annual CyberCitizenship Summit for educators and child safety experts to discuss methods for helping students use technology in positive ways, manage their digital reputations, and help prevent abuse such as cyberbullying.

The company supports the educational work of a number of non-profit Internet safety organizations and associations.

YouTube

Google's YouTube isn't a social network site in the traditional sense, but it is very much a social-media experience as a place online where people establish profiles, channels and playlists, express themselves via video and use both video and text to comment on one another's videos. YouTube uses its own medium (as well as text) to educate users about safety through animated video tutorials.

There is a link to YouTube's safety section at the bottom of its home page. As soon as you land on that page you see and hear a short (1:46) video providing basic guidelines to protect one's safety and privacy with messages that include "don't put up with bullies" and "don't be a bully." The video also advises kids, "If something happens that makes you uncomfortable, tell a trusted adult."

YouTube has additional videos and articles on a variety of safety and privacy subjects including cyber citizenship, privacy, teen safety, hateful content, sexual abuse of minors, harassment and cyberbullying, suicide, impersonation, spam and phishing, and harmful and dangerous conduct.

The company recently instituted a "Safety Mode" tool to give parents and others the ability to filter out potentially objectionable content. Users can turn Safety Mode on or off by clicking on a link at the bottom of any page, and it can be locked into position until the user logs in and enters a password.

YouTube's parent company, Google, provides financial support to a number of Internet safety projects.

SUBCOMMITTEE ON PARENTAL CONTROLS & CHILD PROTECTION TECHNOLOGY

PURPOSE & SCOPE OF SUBCOMMITTEE

According to our authorizing statute, part of OSTWG's congressional mandate was: "*To review and evaluate… the status of industry efforts to promote online safety through… parental control technology, blocking and filtering software, age-appropriate labels for content or other technologies…*" and to study "*the development of technologies to help parents shield their children from inappropriate material on the Internet.*"

The working group's investigation in this and other areas was constrained to some extent by the Paperwork Reduction Act of 1990. Department of Commerce officials notified OSTWG members that we would not be able to solicit input from outside third parties. Consequently, the scope of the review conducted by OSTWG members was limited to those we were able to hear from, what we were able to gather on our own, and our own personal knowledge of these issues and experience in this field.

We were, however, able to personally hear from several leading experts in the field during our meetings together. Among those who presented before the task force on these issues:

- AOL – **Karen Hullenbaugh**, Director of Safety Products
- Common Sense Media – **Todd Haiken**, Senior Manager of Policy
- CTIA–The Wireless Association – **Dane Snowden**, Vice President, External and State Affairs
- Digimarc – **Stuart Rosove**, Vice President for Media & Entertainment
- Entertainment Software Rating Board – **Patricia Vance**, President
- Facebook – **Chris Kelly**, formerly Chief Privacy Officer and Head of Global Policy
- Federal Communications Commission - **Kim Mathews**, Attorney Advisor, Media Bureau, Policy Division
- Federal Trade Commission – **Phyllis Marcus**, Senior Staff Attorney, Division of Advertising Practices
- Internet Safety.com / Safe Eyes - **Forrest Collier**, Chairman & CEO
- Google - **Scott Rubin**, Global Communications & Public Affairs
- Loopt – **Brian Knapp**, Chief Operating Officer
- Microsoft – **Frank Torres**, Director of Consumer Affairs
- Motion Picture Association of America – **Orit Michiel**, Vice President and Domestic Counsel
- MySpace – **Hemanshu Nigam**, Chief of Security
- National Cable & Telecommunications Association – **Rob Stoddard**, Senior VP, Communications & Public Affairs
- Ning – **Jill Nissen**, Vice President, Chief Policy Officer

- RuleSpace – **James Dirksen**, Managing Member
- Symantec – **Marian Merritt**, Internet Safety Advocate
- Think Atomic – **Cheryl Preston**, Brigham Young University Law School
- USTelecom – **Kevin Rupy**, Director of Policy Development
- Walt Disney Company / Club Penguin – **Susan Fox**, VP, Government Relations
- Yahoo! – **Emily Hancock**, Senior Legal Director
- Zynga - **Reggie Davis**, General Counsel

These experts and members of the task force were asked to comment on a variety of questions that the task force was pondering, including:

1. Generally speaking, how well do you think the parental controls **marketplace** (broadly-defined) is functioning? What works particularly well? Conversely, what isn't working so well?
2. How do you measure **effectiveness** in this context?
3. What could be done to generate greater **awareness** or uptake of parental controls or child protection technologies?
4. How do you feel about **default settings**? Should media and technology providers establish more restrictive defaults for their products and services? Should the government mandate or "nudge" providers to set defaults more restrictively?
5. What is the proper **role for government** in this context?
6. What sort of **additional studies and research** would be useful going forward? What questions deserve more study?

After providing a brief sketch of the current market of parental control technologies, a summary of our thoughts and findings about these six questions will follow. Further elaboration and input from various task force members and expressions of minority views can be found in an appendix to the report.

A BRIEF SKETCH OF THE CONTOURS OF THE PARENTAL CONTROLS MARKETPLACE

The parental controls marketplace continues to evolve rapidly in response to changing market realities and needs.[49] A diverse array of parental control technologies exists, and they can generally be grouped as follows:

- **Independent / "Client-Side" Filters and Monitoring Tools:** Until recently, most filtering software was purchased at retail stores or downloaded from websites, and installed on the user's personal computer. These stand-alone or "boxed" filtering solutions are often referred to as "client-side" filters (because in technical terms a web browser is commonly called a "client" that can access content on a web "server"). These client-side

49 A comprehensive and constantly updated list of filter providers and other parental control tools can be found on David Burt's "GetParentalControls.org" blog: http://getparentalcontrols.org/product-guide. Sites such as GetNetWise (http://www.getnetwise.org) provide parents with information and links to filtering programs and educational tools.

solutions are still very popular and many different vendors continue to compete in this market (although some vendors develop for the commercial market while others focus on the consumer market). The market for parental control products is quite deep and constantly evolving with the addition of new tools with a variety of features. These software tools let parents block access to adult content and other problematic websites and typically let parents impose time constraints on their children's computer and Internet usage. Some offer filters that screen certain inappropriate or problematic content based upon the parents' selections or the age of the child. Some only allow access to pre-approved sites, to avoid a problem site getting through the filter. These are called "white lists" or "green lists." Such preapproved lists present a challenge in that new (and unreviewed) content can easily be added to a website. Some tools use technology to screen content on the fly based on keywords and algorithms to block adult and other problem content. These catalogues of prescreened inappropriate sites are called "black lists" or "red lists." Other tools combine the two types of list, and there are challenges for both approaches. While early on human screeners may have been able to handle content review, the exponential increase in user-generated content has made this approach much more challenging and often costly.

Increasingly, standalone products and software packages offer robust monitoring tools that give parents several options, from being able to see each website their children visit, to viewing every e-mail or instant message that they send and receive, to recording their keystrokes, including every word that they type into their word processors or chat conversations, or showing every activity online or on the computer offline. While some products only produce a report accessible on the computer they are monitoring, many of these monitoring tools can even send parents a periodic report by email or text message summarizing their child's Internet usage and communications. More robust software programs even allow parents to capture screen shots of sites their kids have visited, images they send or receive, and other activities.

Some of these products operate for select accounts only – and can be set for children on a child-by-child basis, while others operate for all computer users. Some of these products offer an optional "stealth mode." In stealth mode, once the software is installed on the computer, it is largely invisible to the monitored user and all other users. In open mode, on the other hand, notices may appear when the computer is turned on or the monitored user logs into their account (which can thereby promote dialog between a parent and child about appropriate Internet content). Another option is a tool that permits parents to identify the images that have been accessed on a computer even if the search history has been erased. Some parents find that a child's awareness of this capacity provides incentives for safer online practices.

Filtering is typically obvious to users, as most programs display a message that the site is unavailable due to the filtering or blocking features of the program. Some filtering products, however, merely block the site and the child receives no explanation about why the site cannot be viewed. The child may believe that the site is down, the computer or Internet access is malfunctioning or, should the child be aware of the filter, that it may be blocked. Newer products allow the child to notify their parent or caregiver that they have been denied access to a site and ask their parent to override the filter to allow the site to be viewed, or to change their access permissions from the parent dashboard accessed online from wherever the parent has Internet access.

- **ISP-Integrated Parental Controls and Filtering Tools**: The stand-alone or "client-side" filtering solutions, such as those described above, dominated the online parental controls marketplace in the late 1990s. But the market has changed significantly since then. Today, many Internet service providers (ISPs) and online service providers offer parental control services. These options are usually offered (but not usually provided as a default), to subscribers as part of an integrated suite of security tools, which typically include anti-virus, anti-spyware, and anti-spam tools. These security options are often offered free of charge, or for a small additional fee, when subscribers sign up for Internet service. Some are offered free to all Internet users. Most of these integrated tools offer automatic updates so consumers don't have to manually download upgrades to stay current. Thus, millions of parents now have free or inexpensive Internet parental control tools at their disposal, either through their Internet service provider or other online provider. Of course, parents can also add on other tools or independent filtering and monitoring solutions such as those outlined above.

- **Digital Footprint Searches**: Some services help parents keep track of their children's "digital footprints" by allowing them to search for and view publicly available content posted by and about their children online. These types of tools attempt to collect material from across the web, including public profile information from social networking sites, photo-hosting sites, and blogs or message boards, making it easier for parents to keep tabs on their children's online activity. The reports these services generate can serve as the starting point for important conversations between parents and children about what type of material is appropriate to share publicly, and can help children, teens, and adults get a better sense of what counts as "public" in the online space. Because some online information is not public, these services only provide a partial picture of online information.

- **Operating System Controls and Web Browsers Controls**: Companies such as Microsoft and Apple have integrated some parental control features into their computers' operating systems. The web browsers that these companies offer (Internet Explorer and Safari) work in conjunction with the OS-level controls or other parental control software. Parental control add-ons are also available for the Mozilla Foundation's Firefox browser. Some parental control providers offer a "kid browser" that will give a child their own kid-friendly browser that restricts access to all sites and services aside from those pre-screened and approved for children. These limited kid browsers are much less useful for older children who use computers for research and social interaction.

- **"Safe Search" Engine Filters**: Many major search engines and video-sharing service providers (such as YouTube) offer "safe search" filters that filter objectionable content from search results. This can help block a great deal of content that children might inadvertently stumble upon or intentionally seek during searches. Users are typically allowed to choose from three setting levels ranging from unfiltered to highly filtered. These filters tend to focus primarily on pornography and adult content. This feature may provide an important addition to a parent's Internet management as it can provide filtering of search, which is often not provided by commercial filtering products. Some "safe search engine" filters are not filters at all, however. Some, such as Yahoo! for Kids (formerly known as Yahooligans), offer only preapproved sites in their site pool. The

search engine filters may not block inappropriate images or videos, however, unless the textual description of these media includes keywords identifying them as problematic content.

- **Web Portals for Kids (or "Walled Gardens")**: Many websites restrict content to only that which is appropriate for children. These sites may let kids search for content without the risk of stumbling upon adult-oriented material and help them discover new images, videos, and other kid-appropriate content. They may also help direct children to information and sites that are educational and enriching. In essence, these search portals are massive white lists of acceptable sites and content that has been pre-screened to ensure that they are appropriate for young web surfers. They also provide a safe Web experience for non-readers. To be effective, parental supervision or filtering or other technical tool may be needed to ensure that a child does not navigate away from such websites. One downside of using such services is that a lot of wonderful material available on the World Wide Web might be missed, and children will not be able to discover new sites, content, and games that might have been missed in the massive amount of unscreened Internet content. But many parents may be willing to make that trade-off since they desire greater protection of their children from potentially objectionable content. Concerns have been raised about how appropriate content is selected, how the service handles rapidly-changing URLs and content on previously trustworthy sites, and lack of consistency. Transparency of standards and processes is an important factor in allowing parents to know which site, portal or product to trust.

- **Device / Set-Top Box Embedded Controls**: Many providers of consumer electronics and digital devices now "bake-in" parental control technologies into their hardware. Many video game consoles, DVD players, wireless routers, mobile media devices and phones, cable and satellite set-top boxes, and many other digital devices now include parental control tools. These embedded safety and security tools include: content filtering and screening technologies, time management controls, monitoring capabilities, and blocking tools to restrict access to the web or other users (through "buddy lists"). The primary weakness of these tools is a lack of consistency across platforms; not every device possesses identical capabilities since they are tailored to the needs of specific customers. In addition, using multiple systems and terminologies may be confusing to parents. While widespread protections are not generally available yet in the mobile phone market, parental control products are emerging that allow parents to supervise and control both web and telephone usage on their child's phone.

- **Rating and Labeling schemes**: Several of the technologies mentioned above rely on rating and labeling schemes to trigger filtering mechanisms. Official industry ratings systems—such as the Motion Picture Association of America (MPAA), Entertainment Software Rating Board (ESRB), and Recording Industry Association of America (RIAA) systems – are particularly helpful to technology providers, since they facilitate easier content screening/blocking. Labeling user-generated content is much more challenging, but many websites encourage "community policing" and labeling efforts that let users "tag and flag" the content posted by others in their online community. Site providers or tool makers can then use those "crowdsourcing" efforts to power screening mechanisms. Of course, some sites supplement this with real-time content review, such as porn image detection and review of content textual tags.

HOW WELL IS THE PARENTAL CONTROLS MARKETPLACE FUNCTIONING? WHAT WORKS PARTICULARLY WELL? CONVERSELY, WHAT ISN'T WORKING SO WELL?

Summary

The general consensus from the experts we heard from and from the comments offered by OSTWG members suggested the parental controls marketplace is functioning fairly well for users who understand basic computer security, but that more could be done to improve awareness and usage of existing tools while also striving to improve the tools themselves.

In particular, ease of use is a major concern for some. In addition, several speakers before the task force stressed the continuing challenges associated with the rapid pace of technological change in the Digital Age. User-generated content also presents new challenges for parental control technologies since "amateur" content is ubiquitously available and yet typically not rated or as easy to filter or block (although some filters can block user-generated-content sites entirely).

Discussion

What follows is a synthesis of some of the comments offered by task force members regarding what is and is not working well in this arena currently.

Upsides

Like most areas of the consumer software market, parental controls enjoy robust competition from many companies targeting the same, relatively small market: parents with children old enough to use a computer but young enough to require supervision (although some parents believe all minors require supervision in their online activities).

Software development for the business / enterprise / school segment of the market looking for filtering and monitoring software eventually trickled down to the consumer looking for home solutions, this time targeting parents and their children rather than corporate IT, employees, and students. This competitive market manifests itself in multiple ways, some good and some bad. The upside of this competition is that many products are available, allowing parents to choose software or services that fit their specific needs. That need may boil down to monitoring, filtering and blocking, or some combination of both.

Many major Internet service providers offer some type of parental controls for free. Along the same lines, many broadband providers integrate parental controls into their products and work to educate their customers about their availability and usage.

Some of these basic parental control offerings may have additional value as digital training wheels for kids. One respondent noted that a control as simple as time restriction for Internet usage for younger children not only laid the foundation of boundaries for the child but also established a comfort level for the parent with the feature. As the child grows older, the parent may be more willing to remove the training wheels, so to speak, and ease their children into other forms of media content or communications platforms – and then use a different set of tools to address concerns.

Websites, service providers, toolmakers, and rating organizations have also adapted to changing market conditions. Rating and labeling systems are evolving to account for new forms of content or expression, and have generally become more granular over time, although they are always in a race with evolving technologies and forms of content. Filtering systems are still developing for cell phones with Internet access, portable game players such as PSP, or iPods. The mobile "app" market has

exploded in recent years and the industry is seeking ways to offer rating schemes and new parents controls, although in a somewhat less coordinated way than other industry sectors. Nonetheless, many of the most popular wireless devices now allow application restriction by rating at the phone's operating system level.

Privacy controls are also becoming an accepted – even required – component of online communities and services. As users have demanded more control of their personal data, sites and service providers have adapted to include privacy and data security controls.

Finally, the diversity of products available to parents suggests that there are many kinds of tools available from which parents can choose. It would seem that parents have many different opportunities to utilize various technologies and various approaches to safeguarding their children's media consumption and online experiences.

Downsides
The inverse effect of the product diversity mentioned above is the confusion it creates for the consumer. In this market, that confusion could be exacerbated by the possibility that some consumers are already uncomfortable with the technologies they are evaluating. Some many find it difficult to choose a product, install or activate a program, and maintain it effectively.

Without industry coordination at a higher level, the competing claims made by several products further muddle matters when directed at consumers who may lack the ability or time to sort through competing claims and capabilities. One step suggested by several task force members would be to develop, at the industry level, a centralized website where parents can evaluate parental control solutions using common metrics. For instance, one product may offer filtering, one may offer blocking. To the average consumer those terms may sound interchangeable, but when stacked against each other and other products in the same category, subtle differences emerge.

The limits of technology itself also play a role. The innovative ways in which the Internet and digital technologies have evolved have not been particularly predictable and parental controls will nearly always be playing catch up. Parental control options can both under-block or over-block access to useful information leaving some parents frustrated and leading them to abandon using the product. One suggestion from a task force member was to dedicate resources to develop technologies that incorporate predicted trends. But this is an idea that, by the respondent's own admission, is an expensive and failure-prone proposition.

The Harvard study also noted that: "Filtering and monitoring technologies are ... 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.... 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."[50]

Some task force members were concerned about the narrow focus of the industry on the home PC relative to other devices or methods of accessing digital content. In the last few years, wireless access points have exploded, with nearly any device imaginable becoming wirelessly connected to the Internet, from mobile phones to video game consoles to refrigerators. Many worry that the scope

50 Internet Safety Technical Task Force, *Enhancing Child Safety & Online Technologies: Final Report of the Internet Safety Technical Task Force to the Multi-State Working Group on Social Networking of State Attorneys General of the United States*, Dec. 31, 2008, at 153, http://cyber.law.harvard.edu/pubrelease/isttf.

of available software for new devices or platforms is too narrow or that parents are not adequately informed about how to take advantage of existing solutions.

One thing that the current parental controls technologies handle less well is Web 2.0 or user-produced content (including content created by kids). This affects older children who frequent social network sites in particular, since current software solutions typically only offer a pass / fail (allow or block) option when confronted with something like the dynamic content on a social network site. That binary choice may be undesirable, and potentially unworkable, for parents of increasingly social teens.

Lack of sufficient product integration is another area where some argued there was room for improvement. Some respondents note that parental control tools sometimes appear to be tacked on as an afterthought at the end of a product's design process. Parents are sometimes unaware of the options and how to locate and activate them on any given service or product. A unified, ground-up approach in which parental controls are a core piece of the product's construction would be welcome. Of course, even if they are "tacked on as an afterthought," many of those tools can still be quite effective.

Finally, the very term "parental controls" is problematic to some. Given the various methods by which these parental control software products work, more specificity could be warranted to reduce confusion on the part of parents. For example, blocking software and monitoring software would probably fall under the label of "parental controls" but each does something very different. Were a parent to choose one over the other blindly, there may be a false sense of security that harmful content is being blocked from the machine when that is not always the case. As a component of the call for more education, a shift from a catch-all term for a diverse spectrum of software could be appropriate.

HOW DO YOU MEASURE EFFECTIVENESS IN THIS CONTEXT?

Summary
Measuring effectiveness and success in this arena remains a controversial topic. The experts on our task force and those presenting at our meetings had varying definitions and metrics regarding the effectiveness of parental control technologies and rating and labeling systems. And the issue is complicated by the nature of the marketplace, where the available technologies, content, and parental demand and concerns are always in a state of flux.

Discussion
Measuring effectiveness requires more than simply collecting and tallying data, because determining what is "effective" necessarily involves some value judgments. Some online safety task forces have attempted to incorporate evaluations of various approaches and technologies.[51] The OSTWG task force did not possess the resources to conduct a similar review, and, as noted above, our efforts were limited by the confines of the Paperwork Reduction Act.

However, to the extent evaluation of effectiveness is conducted by future task forces or working groups, several OSTWG respondents offered up potential criteria for evaluating effectiveness. Among them:

51 See: Computer Science and Telecommunications Board, National Research Council, *Youth, Pornography and the Internet* (Washington, DC: National Academy Press, 2002), www.nap.edu/html/youth_internet and Internet Safety Technical Task Force, Enhancing Child Safety & Online Technologies: Final Report of the Internet Safety Technical Task Force to the Multi-State Working Group on Social Networking of State Attorneys General of the United States, Dec. 31, 2008, http://cyber.law.harvard.edu/pubrelease/isttf.

- Ease by which parents can find products and services they need
- Efficacy of each tool to do what it claims to do
- Likelihood that parents to effectively deploy a product to address a perceived need
- Sufficient labeling of minimum system requirements to run a product
- Ability of parents to understand how a product interacts both with the machine and with users
- Flexibility of a product to deal with the progressing age and skills of the child
- Disruption that products cause to acceptable Internet activities
- The likelihood that use of the parental controls were abandoned for being ineffective, too hard or not fitting the family's needs

Another factor to consider, as discussed above, is that measuring the uptake of parental control software may not provide a complete picture of parental involvement in their children's Internet usage. Several respondents noted that many families choose many methods other than technology to monitor or control their children's media and Internet usage. Statistics regarding the number of students who learn about Internet safety at school would also be a valuable metric in assessing the effectiveness of strategies designed to keep children safe online.

WHAT COULD BE DONE TO GENERATE GREATER AWARENESS OR UPTAKE OF PARENTAL CONTROLS OR CHILD PROTECTION TECHNOLOGIES?

Summary
There was a great deal of agreement among the experts we heard from as well as the OSTWG members that industry, researchers, government, and other organizations can take more steps to expand awareness about parental empowerment technologies. Comments along these lines were typically grouped into three sets of recommendations: (1) Engaging parents and kids in greater conversation; (2) Increasing general education and awareness efforts and campaigns; while (3) Improving the quality and ease-of-use of the tools themselves.

Discussion
Respondents were generally in agreement about the major requirements to increase awareness, and potentially uptake, of parental software. First, engage the consumer. Ask parents what they need and what they are looking for from a parental software product and manage the false expectation that once the parent installs this product on their home computer their child is now "safe" on the Internet. As part of this process, also engage children. Find out what they are using the Internet for, at progressive age levels, and determine how products can help enforce parental boundaries while not detracting from the usefulness of allowed websites. Some respondents suggested highlighting the positive content that these tools will allow children to see, rather than emphasizing all of the questionable content the tools will keep out; however, others felt that parents may not sufficiently understand the risks and underestimate the need for supervision of children online. Along similar lines, emphasize that parental software is just one tool in a parent's hand, not a replacement for supervision and active participation in their children's online experiences.

Second, educate the consumer. Reach out via the media with positive campaigns emphasizing what properly supervised children can accomplish academically and socially with Internet access. High-volume Public Service Announcements are typically effective at creating awareness, and industry best-practice guidelines would help standardize what parents can come to expect from parental software

and reduce consumer confusion. Some respondents suggested that legislation earmarking funds for consumer education and digital literacy campaigns would be helpful, and others suggested that devices used to connect to the Internet (such as game consoles) could come with highly visible labels informing parents that the device could be used to access the Web.

HOW DO YOU FEEL ABOUT DEFAULT SETTINGS? SHOULD MEDIA AND TECHNOLOGY PROVIDERS ESTABLISH MORE RESTRICTIVE DEFAULTS FOR THEIR PRODUCTS AND SERVICES? SHOULD THE GOVERNMENT MANDATE OR "NUDGE" PROVIDERS TO SET DEFAULTS MORE RESTRICTIVELY?

Summary
Default settings—or how parental controls are configured "out-of-the-box" by vendors or website operators—are another controversial topic. The experts and OSTWG members we heard from had differing views on how parental software defaults should be set and who should set them. And because there is such a broad diversity of sites, services, content, and applications that must be considered, the wisdom of default settings can only really be considered by narrowing the scope of focus.

Generally speaking, however, most agreed that the government should not be in charge of establishing the defaults. The controversy came instead from the question of whether content creators and distributors should voluntarily set defaults more restrictively and then let parents "opt-out" of those settings. Or, alternatively, if they should simply provide clear and unambiguous notice of the parental empowerment technologies available and let parents "opt-in." Several participants, however, stressed that setting defaults too restrictively could create confusion or hamper the user experience unnecessarily. Some participants believe that setting reasonable defaults (with notice that more and less restrictive options are available) would be helpful.

Discussion
Respondents generally agreed on two ideas:

1. Default settings should be given careful consideration before shipping a product because they typically go unchanged after the fact; and,
2. Government intervention to establish default settings is undesirable for several reasons.

To the first point, default settings should be carefully considered during the product design phase, and a product should be evaluated based heavily on how it performs out-of-the-box, given that most consumers do not alter the default settings on technology products. To mitigate this behavior, there were suggestions such as ensuring that products were set to "non-stealth" mode by default or that they would launch with a set-up wizard to guide parents through the choices that are available to them, rather than keeping the default settings buried in a menu that some parents may have difficulty finding.

Some voiced the opinion that since settings can ultimately be changed, why not simply default them to the most restrictive possible? Others countered that if a product is too restrictive out of the box it would block content to the point where many would complain that the product is "broken" and the potential for abandonment would increase. A median suggestion was to invest in research to determine a level of restriction that is neither too loose nor too restrictive, and combine default settings with education about changing the defaults.

Several respondents echoed similar opposition to government intervention in mandating the

restrictiveness of default settings. Government-mandated default settings, which would serve to restrict access to information, may raise First Amendment concerns. Another argument against mandated defaults is the inability of government to act quickly enough to keep up with the speed at which the Internet and digital technologies evolve. What may be considered a threat today may be benign tomorrow or vice versa, and if the industry were handcuffed by a requirement for rigid settings, the likelihood of a product's adoption and ultimately control tool companies' ability to do business would suffer.

One suggested compromise would be an agile, evolving set of industry best practices developed through collaboration between industry, NGOs, and government, which could serve as common ground while also adapting to changes in the landscape.

WHAT IS THE PROPER ROLE FOR GOVERNMENT IN THIS CONTEXT?

Summary
The OSTWG members and experts we heard from offered a smorgasbord of useful suggestions regarding how government could help in this area. Generally speaking, however, most were not keen on the government playing a greater regulatory role. Instead, education, funding, and empowerment strategies tended to be at the heart of most of the recommendations.

Discussion
Funding and a light touch when it comes to any type of mandate was the nearly universal reply from panelists to this question. Among the endeavors that would benefit from government funding include: digital literacy programs, public service announcements, and public school curriculum.

Tax incentives for companies to encourage product innovation or to bring themselves into voluntary compliance with best practice guidelines was one suggestion, as was additional law enforcement funding earmarked for Internet-related matters.

Other suggestions included adoption of a set of national goals in the space of online child safety to guide the industry, along with funding to engage the public health sector in the area of at-risk youth in the online setting.

WHAT SORT OF ADDITIONAL STUDIES OR RESEARCH WOULD BE USEFUL GOING FORWARD? WHAT QUESTIONS DESERVE MORE STUDY?

Summary
Task force members and the experts we heard from all agreed that more research would be helpful in determining what does and does not work in this area. Several experts spoke of the need for a better "gap analysis" to determine the tools and approaches needed to address existing or emerging concerns. While the Pew Institute and others devote substantial resources to these studies on an ongoing basis,[52] there may be need to study issues with a more precise focus.

Discussion
Among the suggested areas of additional study:

- Technology adoption and use in the home by age of child
- Technology adoption and use in the context of the US educational system

52 See supra note 3, for instance.

- Parental control software adoption and use in the home by age of child
- What the major impediments are for parents who don't use parental controls
- Parents' goals in using technology tools to help protect, supervise, and monitor their children by age of child, and how they differ with those of a child.
- Long-term effects of differing methods of parental supervision and communication with and without using parental control software technology by age of child
- Parental concerns and awareness of online safety risks
- Impartial benchmarking and testing of parental control software
- Parental control software products currently under development
- Identification of online risks for youth by priority and age
- Short and long-term effects of encounters with age-inappropriate or potentially offensive content online and other risky behavior
- Short and long-term effect of education programs on the mitigation of risks that youth face online
- Unique safety concerns with "at-risk" youth in an online setting and how best to address them

GENERAL CONCLUSIONS & RECOMMENDATIONS REGARDING PARENTAL CONTROL TECHNOLOGIES

Generally onsistent with what other online safety task forces have found, with regard to parental controls technologies, the majority generally concluded that:

1. **There is no single "silver-bullet" solution or technological "quick-fix"** to child safety concerns. That is especially the case in light of the rapid pace of change in the digital world.
2. **Empowering parents and guardians with a diverse array of tools**, however, can help families, caretakers, and schools to better monitor or control online content and communications.
3. Technological tools and parental controls are most effective as part of **a "layered" approach to online safety** that views them as one of many strategies or solutions.
4. The best technical control measures are those that work in tandem with educational strategies, parental involvement and approaches to better guide and mentor children to make wise choices. Thus, **technical solutions can supplement, but can never supplant, the educational and mentoring role.**
5. **Products and services need to be designed with the families' needs in mind,** allowing parents to use the right settings and the right tools for their need and adapt to changing needs. Parental control technologies **have to be easy to use, accessible, flexible, and comprehensible for the typical parent.** They need to provide different features for the varying needs of all the children in the household.
6. **Industry should continue to formulate and refine best practices and self-regulatory systems** to empower users with more information and tools so they can make appropriate decisions for themselves and their families. And those best practices,

which may take the form of an industry code of conduct or default control settings, should constantly be refined to take into account new social concerns, cultural norms, and technological developments.

7. **Government should avoid inflexible, top-down technological mandates.** Instead, policymakers should focus on encouraging collaborative, multifaceted, multi-stakeholder initiatives and approaches to enhance online safety.
8. **Additional resources for education** and awareness-building efforts are absolutely crucial.
9. **We must engage our youth in constant dialogue** and always be willing to talk to them about difficult issues, challenges, or content they face online.

SPECIFIC RECOMMENDATIONS ON PARENTAL CONTROL TECHNOLOGIES

Content creators, digital device providers, website administrators, and network providers should:

1. **Engage in ongoing awareness-building efforts:** The more education and awareness-building the better. Improved product descriptions, tutorials, and other forms of user assistance are vitally important.
2. **Promote greater transparency:** Users/parents should be given a clear understanding of what sort of content and information they will come in contact with when they or their children use certain media products or visit certain websites and use features allowing them to communicate with third parties or share information.
3. **Parental empowerment technologies and options should be included in new offerings whenever possible:** "Safety by design" should be encouraged and companies, sites, and services should "bake in" safety tools and settings whenever and wherever possible. Greater industry collaboration and common approaches are also encouraged.
4. **Enable and promote "community policing":** Social networking sites and other sites that host user-generated content should utilize, improve, and expand "community policing" capabilities. Reporting mechanisms should be established and refined to ensure problems are dealt in a timely fashion.

PARENTAL CONTROLS TECHNOLOGY SUBCOMMITTEE: ADDENDUM A

SURVEY OF OSTWG MEMBERS AND PRESENTERS ON THE STATE OF PARENTAL CONTROLS & CHILD PROTECTION TECHNOLOGY

OSTWG members and the experts we heard from were asked to comment on a variety of questions that the task force was pondering, including:

1. Generally speaking, how well do you think the parental controls **marketplace** (broadly-defined) is functioning? What works particularly well? Conversely, what isn't working so well?
2. How do you measure **effectiveness** in this context?
3. What could be done to generate greater **awareness** or uptake of parental controls or child protection technologies?
4. How do you feel about **default settings**? Should media and technology providers establish more restrictive defaults for their products and services? Should the government mandate or "nudge" providers to set defaults more restrictively.
5. What is the proper **role for government** in this context?
6. What sort of **additional studies / research** would be useful going forward? What questions deserve more study?

A sampling of some thoughts and findings about these six questions follows.

HOW WELL IS THE PARENTAL CONTROLS MARKETPLACE FUNCTIONING? WHAT WORKS PARTICULARLY WELL? CONVERSELY, WHAT ISN'T WORKING SO WELL?

Upsides (or What's Working Well)

- "The parental controls marketplace is, like many markets, a collection of companies vying for a relatively small audience (e.g., parents with children of a specific age group). In one sense, this creates healthy competition among the players which generally produces better results in terms of feature sets than regulated markets. On the other hand, it can be confusing for a parent to determine *which* tools are the best for their specific situations. It can sometimes be difficult to sift through the marketing hype to make a decision that suits your own needs and parenting styles. Also, there isn't a 'magic bullet' solution that covers all aspects of parental controls in all situations." – ***Holly Hawkins, AOL***
- "I do think that the parental controls marketplace offers a fairly wide range of tools that can be used to enhance child online safety – whether integrated features of online products and services or as standalone solutions." – ***Elizabeth Banker, Yahoo***
- "There are many product choices and the technology is quickly advancing—seems like the market is functioning well. The industry is increasingly competing on privacy and security, and improvements in these areas spillover in the child context. However,

markets function best when consumers have a high degree of product awareness and education. Unfortunately, there's more to be done to make parents more aware of the technology tools they have at their disposal, and how best to use them for their desired effect." – ***Braden Cox, NetChoice***

- "USTelecom believes the parental control marketplace is functioning extremely well. What is working particularly well is that parents today have numerous choices and tools to choose from in ensuring their children have access to a safe media environment. Additionally, many wireline broadband providers are actively educating their customers on the availability and benefits of tools available through their online and/or video offerings (*e.g.*, DVRs, Parental Control online tools, etc.). Many wireline broadband providers are also directing their customers to additional, third-party resources for keeping their kids safe online." – ***Kevin Rupy, USTelecom***
- "The marketplace *per se* is working well. There appears to be no shortage of software solutions, and most major ISPs offer complimentary parental controls packages to their subscribers." – ***Rob Stoddard, National Cable & Telecommunications Association***
- "One feature of parental controls we find used regularly is internet access time limits for the younger children. Including the software for free with a service makes the choice easier for parents to try. Parents who have started in the early years getting involved in their children's online activities and attempt to keep up with the technology find it easier to be a part of the child's online activities in older years." – ***Jay Opperman, Comcast***
- "Ning has… found that giving users (parents AND children) the opportunity to police or 'govern' their own communities by providing them with the appropriate community management tools to do so and educating them on how to use them is extremely powerful. It is very effective when someone is empowered to take ownership of their community – they want the community to be safe. The community will police itself when they feel that they are actually a part of it." – ***Jill Nissen, Ning***
- "We want a variety of solutions in the marketplace because there is such a huge diversity in user needs. It is not clear to me that a significant percentage of parents are asking for parental control technology that does not exist in the marketplace." – ***Brian Markwalter, CEA***
- "Wireless carriers offer a plethora of parental empowerment tools, including but not limited to, content filters, calling and text limits, camera function limits, parental notifications, pre-approved calls, and purchase limitations. Wireless carriers also voluntarily adhere to CTIA's Carrier Content Classification and Internet Access Guidelines. Wireless manufacturers offer a variety of built-in parental empowerment tools, such as password protected function and feature limits. In response to the burgeoning wireless applications ("apps") market, manufacturers are also developing or offering content rating and filtering tools. Third party vendors offer a variety of downloadable parental empowerment tools including device monitoring, parental notifications and content filters." – ***Dane Snowden, CTIA***
- "Game consoles and handheld devices are highly effective at blocking by ESRB rating. Certain game consoles are highly effective at providing a parent with the ability to manage whom their children can play with online, and in some cases when and for how long. Many offer restrictions on access to online content and offer helpful guides on how these settings can best meet a parent's individual needs. That being said, no single tool or set of tools will solve the "digital divide" between those households who care about being proactive about Internet safety and those who don't." – ***Patricia Vance, ESRB***
- While there is a great deal of confusion around parental controls, there are some things that are working well. There are a variety of tools that are free or affordable. Parents, once they know what to look for, can find the right product to fit their needs and tech skill levels. The industry has been very responsive and better approaches, features and technologies are made available frequently. The industry and providers often combine educational tips with their parental controls which makes the tools relevant and helps parents make the right choices. Privacy settings are now accepted practices and users can typically block strangers and known harassers from being able to communicate with them online. Unlike the early days of parental controls in 1995, parents can find what they need, often for free, through a simple search online or by viewing their provider's help or safety pages. - ***Parry Aftab, WiredSafety***
- "What makes the parental control approach work is the diversity of tools available, both in terms of what the tools do (monitor, filter, etc.) and in terms of what types of content the tools allow parents to control. Families that want very strict controls will find options, as will families that instead seek looser controls that only address the most extreme content. And as children grow up, the tools available can evolve and grow with them. And more broadly, there is significant competition in the marketplace." – ***John Morris, CDT***

Downsides (or What's Not Working So Well)

- "There is no industry coordination, everyone is doing their own thing. There are vastly overblown claims, parents don't know which to believe. There is no central site/service to highlight all of them and show the differences." – ***Parry Aftab, Wired Safety***
- "The potential dangers our children face through their use of technology is changing faster than software makers can keep up. Much like the malware marketplace, vendors are always a step behind latest threats. The best parental controls providers can do is to anticipate how kids will be using technology in the future, and take risks on investing in products to meet that future need." – ***Holly Hawkins, AOL***
- "The parental controls marketplace functions well under some very specific and limited circumstances, but it is inadequate in other essential areas. While we recognize many improvements in products over the last five years, most parents remain overwhelmed with the task of managing their family's Internet experience, particularly parents with older youth. The parental controls marketplace works well for managing content for young children who use a limited number of connected devices. Where iKeepSafe envisions improvements is in the protection for older children who want to participate in the web community. It's very hard for parents to manage the Internet experience of older youth when they need to be on sites that cannot be filtered adequately. One primary, glaring hole in the parental controls marketplace is the lack of a plug-and-play, pre-filtered Internet service, suitable and affordable for consumers, where filtering occurs outside and independent of the home computer. Many products exist that adequately—not perfectly—filter content unsuitable for children. Another hole in the marketplace is in the parental controls for Web content available through cell phones. While many providers offer filtering and monitoring software, most parents either don't know they exist or don't know how to use them." – ***Marsall Hancock, iKeepSafe***

- The parental controls market does not effectively manage Web 2.0 content. Kids want to be where they can share content: Norton identified YouTube, Facebook and Google as the top three searches for kids. Social networking, virtual worlds, gaming, and media sites where user-generated content is uploaded are difficult to filter by individual user. Within some of these sites, improvements have been made to regulate content by allowing users to flag inappropriate content. Even with these improvements, parents still struggle to provide a managed Internet experience for children in these sites. Many parents feel that the only secure way to block inappropriate content in these venues is to block the sites entirely. iKeepSafe does not see this as a realistic solution. – ***Marsali Hancock, iKeepSafe***
- "Certainly, there is a plethora of products. The sheer quantity of competing products may actually contribute to the despair parents feel when trying to make intelligent decisions. Some kinds of uniform standards of measurement and required disclosures would be extremely helpful. Although many of these parental control options offer some meaningful protections, none are sufficient and it would be misleading to suggest the only difficulty is choosing among existing offerings. "The most commonly reiterated concern of members of OSTWG was that parents are not satisfied with what they perceive to be the options. Of course, this problem may be mitigated with a coordinated education effort, but we did not begin to formulate a feasible scheme for getting the information to parents." – ***Ralph Yarro, Think Atomic***
- "Industry does provide some parental controls, and filtering, but they could make it much easier to find these features on their pages and much easier for parents to understand and use. While they may provide it, parent controls and child safety need to be a top priority. One of the challenges with the Internet is that there is currently no way to separate out inappropriate content from content that is appropriate for children. Filters can be used and are certainly helpful, but they're not child-proof. Many parents know they should be using filters, but are not for various reasons. ISPs should have a duty to protect children from the potential harmful effects of the internet." – ***Jeremy Geigle, Arizona Family Council***
- "Many parents are not aware of the products that are available. There is no standardization among products in their use, so "parental controls" on one system operate differently than parental controls on another system, and makes it much more difficult for users." – ***Hedda Litwin, NAAG***
- "Parental controls and utilities are only effective to any degree when they are being used. That initial and paramount hurdle is one that has not yet been effectively overcome. Eventually this problem will resolve itself as people who grew up using computers and the Internet become parents themselves, but in the interim more outreach to parents would be welcomed. As important as the message itself is, the medium through which it is delivered is crucial to success. Often this message is delivered through the Internet itself, perhaps through safety oriented organizations. This can be an effective however the parent most in need of information is the parent who likely doesn't even know they need it. Putting the information where parents can easily access it, be it via television, print, or radio, would be a measure that could help soften the narrowing gap between once intimidating technology and a parent's participation in their child's internet activity." – **Hemanshu Nigam, MySpace**
- "Many parents are still not aware of the various products out there. Better adoption appears to be when incorporated for free into a product or part of the product offering from the start (i.e. the various granular privacy and safety options available on sites such as Ning, Facebook, MySpace, etc.)." – ***Jill Nissen, Ning***
- "A parent's decision not to employ parental controls in his or her home, be it proactive or passive, may be due to a variety of reasons, including but not limited to: 1) lack of awareness of the tools available; (2) lack of concern or awareness about the risks associated with his/her child's use of the Internet; (3) lack of sophistication in many tools to account for individual tastes, values, concerns or age of child – and for those tools that are more sophisticated, lack of ability or interest in spending the time and effort to set them up; and (4) inaccessibility of the device in the child's possession or bedroom. We need to better understand what motivates a parent to use such tools and why many don't use them today." – ***Patricia Vance, ESRB***
- "[M]ore work must be done to develop and implement parental controls for social media applications across all platforms." – ***Rob Stoddard, National Cable & Telecommunications Association***
- "Probably adequate but it could be better…sometimes it feels these are bolt on capabilities versus something that is thought of as core to the service." – ***Jay Opperman, Comcast***
- "The marketplace is a bit confusing. For example, even the term 'parental controls' is a catch-all encompasses many different kinds of software functions that aren't included in every software package. There are different functions and expectations for safety using different software tools—filters, blocking, monitoring, etc.. This can cause confusion for parents." – ***Michael Kaiser, National Cyber Security Alliance***
- "As technologies evolve and new ones emerge, the tool makers will necessarily have to work to keep up. Most tools regularly release updates and new filtering lists, but no tool will ever be perfect. But that is true of the vast majority of child safety tools in our society – from car seats to bike helmets." – ***John Morris, CDT***

HOW DO YOU MEASURE EFFECTIVENESS IN THIS CONTEXT?

- "The base measures of parental controls effectiveness are adoption, tenure, and satisfaction. If parents aren't adopting, using, and happy with their chosen parental controls product, then it is not effective. Factors influencing parental controls product success include ease of use (install, set up, configurations), breadth of features, use across devices (single PC, network, mobile devices, etc.), and time commitment necessary from parent to manage controls. Another factor is the relevance of the product to the age of the child in question. A child of 5-7 is going to use technology much differently than a teenager, and tools that are effective for one are not necessarily effective for the other." – ***Holly Hawkins, AOL***
- "In terms of effectiveness of such tools, it appears that there is still some resistance to wide-spread use of such tools and that the gap may be due to a lack of knowledge on the part of parents and other responsible adults or a lack of engagement in kids and teens online behaviors. Lack of use of even really great tools that do exactly as promised should probably be considered when looking at the status of such tools and what they currently add to the child safety effort. However, I do not think that lack of use should be taken as a reflection on whether or not the technology is where it needs to be. It's kind of like a seatbelt only working if you buckle it – that's not a flaw with the seatbelt." – ***Elizabeth Banker, Yahoo***

- "You have to ask parents. Is it working the way it is? (The answer is a resounding "no!" for the thousands of parents I speak with each month.) So, we have to ask them about their needs. When products are too complicated for parents to use effectively, they abandon them. Many product providers shoot from the hip. They address the needs of one demographic group, ignoring others, are very value-based or overly-complicated to avoid being value-based, and make assumptions about parents as a whole, just because they have children themselves. They don't know their markets as well as they should and have a large failure rate." ***– Parry Aftab, Wired Safety***
- "We measure effectiveness based on several factors: (1) How likely are parents to find the product/service? (2) How likely are parents to have the necessary skills to implement the product/service effectively at home? (3) How often is the parent's routine disrupted by the service? How many times a day does a child request access to a legitimate site because of parental control interference? Does the product slow or impede the online experience for the adults in the home? Does the machine used in the home have sufficient memory to run the product effectively? (4) Can the parent meaningfully engage in what the child is doing online in terms of content viewed, contact with other users, and conduct within Web communities? Can parents effectively manage the Internet experience as the child ages, ramping them into responsible digital citizenship?" ***– Marsali Hancock, iKeepSafe***
- "This is a difficult question. Since for each type of software there are different measures, we need to establish effectiveness by type (blocking, filtering, monitoring, etc). A stronger consensus around what effectiveness means would be helpful as well. One clear measure is consumer satisfaction. Does the product, in their experience, actually do what it promises, and do parents feel that their children are safer as a result." – ***Michael Kaiser, National Cyber Security Alliance***
- "Two prongs to measuring effectiveness. (1) The first is to measure the number of young people in our school systems that are being taught internet safety. Just because they know about the dangers doesn't mean that they won't intentionally place themselves in danger, but it at least gives us a quantifiable measurement of those being taught about the danger. (2) Gauge the number of young people (and adults) who are successfully using internet safety education to avoid inappropriate content." ***– Jeremy Geigle, Arizona Family Council***
- "It is critical to differentiate between a measure of effectiveness for a given product, such as a filtering program, and a measure of effectiveness for the entire concept of user or parental empowerment as an approach to online child safety. With regard to individual products, the federal judge who decided the COPA litigation received extensive evidence from expert witnesses, and found that the leading filtering tools were highly effective at blocking out unwanted sexual content – far more effective than the COPA law being challenged in that case. The filtering tools were able to block 90% of more of such content. Looking more broadly, however, the question of societal uptake of filtering tools is *not*, in my view, a good measure of the effectiveness of the user empowerment approach to online safety. Many families choose methods other than technology to supervise and guide their children's online experience. More effort to promote awareness of technical tools is certainly desirable, but the fact that many families do not install filtering software does not indicate that user empowerment is not an appropriate approach to online child safety." ***– John Morris, CDT***

- "Data of consumer awareness and attitudes toward available control tools and services developed by an independent and reputable organization. Independent non-governmental review bodies to determine that available content tools meet consumer expectations." ***– Dane Snowden, CTIA***
- "Measure usage of the controls. Surveys of satisfaction with the parental control tools." ***– Hedda Litwin, NAAG***
- "There is a need for more research on consumer awareness and use of the broad array of parental controls and tools available today, and particularly to gain insight into *why* those parents who are aware of parental controls choose not to use them. We also need to better understand consumer satisfaction with the tools in use, by reviewing consumer feedback and conducting consumer research. Moreover, the efficacy of tools to do what manufacturers say they do should be evaluated." ***– Patricia Vance, ESRB***
- "Public opinion polling could be utilized to measure awareness, usage, and effectiveness of parental controls. In addition, consultation with ISPs, internet companies, law enforcement officials, and other stakeholders, to identify potential reporting and tracking mechanisms for the volume and trending of concerns or complaints, might be useful." ***– Rob Stoddard, National Cable & Telecommunications Association***

WHAT COULD BE DONE TO GENERATE GREATER AWARENESS OR UPTAKE OF PARENTAL CONTROLS OR CHILD PROTECTION TECHNOLOGIES?

Importance of Talking to Parents & Children / Encouraging Constant Engagement

- "Start with the parents. Ask them what they need and make it easy for them to use the products, make them relevant and not overwhelming. Manage expectations. They often think they can set it and leave it. But effective tools require tweaking and rethinking, as well as moving the bar when the kids become older and better able to protect themselves. Also, get kids and teens involved." ***– Parry Aftab, Wired Safety***
- "Talk to parents AND children. One thing that Ning has done is really engage our members and Network Creators and get their input on what is and what is not working with the tools that they have to control their privacy and safety and moderate their social networks." ***– Jill Nissen, Ning***
- "I think the continued struggle is how to get parents and other adults more engaged in what kids do online. Frankly with the proper level of engagement, such as parents who talk to their kids about what is and is not okay to do on Facebook, the tools are probably a lot less important. I'm not sure exactly how to do this, but we have seen several fairly negative campaigns designed to motivate parents with fear and I think trying something more positive may reach the audience who has not responded to fear-based messaging." ***– Elizabeth Banker, Yahoo***
- "Software is no substitute for supervision by a parent or guardian or for open communication with children and teens. Because parents cannot always be present when their child is online, filtering and monitoring software can be a valuable tool, but it cannot guard a child from potential risks that exist online. It is always important to remember that an Internet filter is a tool and is no substitute for your supervision or for regular communication with your children or teens." ***– John Shehan, NCMEC***

General Education / Awareness-Building Efforts

- "Get the word out – there is still a lot of misinformation about the technologies and what they can and can't do. Be positive in conveying the real message and debunk the urban legends." – ***Parry Aftab, Wired Safety***
- "A national media literacy campaign targeting different audiences (i.e., younger kids, teens and parents/caregivers) could help to raise awareness of the tools and practical steps each can take to address Internet safety concerns. Government, NGO's, associations (ALA, PTA, etc.) and industry members can also help raise awareness and distribute educational materials on digital literacy." – ***Patricia Vance, ESRB***
- "A national campaign by the Ad Council might help generate more awareness to parents that these types of products are available – and often at low or no cost from their ISPs. Internet service providers could also do more to highlight the parental control products that they have available to their users, and how the users can benefit from using the products. This type of information is often buried in lower levels of their sites." – ***Holly Hawkins, AOL***
- "More focus on technology tools, less focus on fear. Encouraging technology reporters to cover parental control technologies and do occasional product reviews. Get a legislator or prominent community official to speak about parental controls. Industry needs to continue to get the word out. Educators can involve parents." – ***Braden Cox, NetChoice***
- "Cooperative efforts by industry, non-profit organizations and government are ideally suited for increasing awareness amongst consumers and parents to increase uptake of parental control technologies." – ***Kevin Rupy, USTelecom***
- "With regard to children, federal and state education policy should encourage the integration of digital literacy and responsible use courses to ensure children are positively using new technologies. With regard to parents, online safety advocates should engage on parental empowerment campaigns and encourage parents to effectively use available tools and services. With regard to industry, governmental entities and online safety advocates should continue to partner with industry to focus on specific issues and trends." – ***Dane Snowden, CTIA***
- "Companies that benefit from the internet could do more to develop, promote and market effective parental controls every time they sell their products. Awareness and education for parents is much needed to help shield children from inappropriate material online. Possibly "warning" labels on devices that access the internet, to alert parents. Local, state and national classes, online classes, online ads, public service ads, explaining the possible harms a child could encounter online and a parent's role to protect their children. Media statements, media interviews, and media blitz that bring this issue to people's attention. Industries should better promote their parental controls -- again, make them easier to access and use. If we educate the parents, it seems there would be a natural consumer demand for industries that cater to parents and online safety for children." – ***Jeremy Geigle, Arizona Family Council***
- "(1) Public service or other national campaigns to raise awareness of the various options. (2) Distribute "best practice" guides for various industries (i.e. settings for social networking sites, etc.) in schools to both teachers and children and use these guides to educate on how to stay safe online by actually using the technologies instead of just banning the use of them in schools. This should be incorporated as part of the regular curriculum (i.e. during a computer class). (3) Make it easier for parents and children to locate and understand the various options (controls or settings) available to them on the various services (i.e. Safety Tips and Resources easily accessible, etc.). (4) Peer to peer training." – ***Jill Nissen, Ning***
- "Traditional public service campaigns - with simple messages repeated at a high frequency - are always useful. However, any consumer education initiatives on this topic should focus extensively on infiltrating online services and content and should be designed to spread virally, in order to best reach the intended audiences." – ***Rob Stoddard, National Cable & Telecommunications Association***
- "Certainly, publicity campaigns and educational efforts are admirable, but would be enormously expensive to create and coordinate at the level necessary to give a substantial number of parents the information they can effectively use." – ***Ralph Yarro, Think Atomic***

Improving the Quality of the Tools / Better Industry Coordination

- "These products tend to be all about 'no.' Parents (and the kids) need to be taught to see these as empowering, not the cyberpolice. The products should steer the users to good resources, sites and networks." – ***Parry Aftab, Wired Safety***
- "Improvement in product solutions would increase uptake. Parents do not have a viable option for providing the type of Internet that they experience at work–pre-filtered, that requires no setup from home, and that cannot be worked around by savvy kids." – ***Marsali Hancock, iKeepSafe***
- "Enclosing disclosure statements on or with any Internet facilitating product or web-enabled device that warns parents of capabilities of the product and the limited nature of optional controls may be helpful." – ***Ralph Yarro, Think Atomic***
- "The industry could come together to find ways to better characterize their products, find some common language for educating parents, establish some benchmarks for product effectiveness and quality, and establish some best practices that would be shared across the industry depending on the function of their product." – ***Michael Kaiser, National Cyber Security Alliance***
- "Apart from the aforementioned use of more traditional media to gain access to parents who don't necessarily use the World Wide Web with great skill, another strategy would be closer integration with technology at the device or operating system level. Rather than a third party piece of software that must be discovered, purchased, and installed, some companies have already found some success by integrating parental controls into devices, commonly the case with cable television boxes and digital video recorders for example. The Internet Service Provider level is another logical point to integrate some type of parental controls." – **Hemanshu Nigam, MySpace**
- "Standardize the usage of some of the parental control features so users don't have to learn new systems each time they change hardware; also one simplification manual could be used for all." – ***Hedda Litwin, NAAG***

HOW DO YOU FEEL ABOUT DEFAULT SETTINGS? SHOULD MEDIA AND TECHNOLOGY PROVIDERS ESTABLISH MORE RESTRICTIVE DEFAULTS FOR THEIR PRODUCTS AND SERVICES? SHOULD THE GOVERNMENT MANDATE OR "NUDGE" PROVIDERS SET DEFAULTS MORE RESTRICTIVELY?

- "Behavioral economics informs us that defaults matter—a lot. Most consumers will not change a preselected default setting even when given the option to do so. Media and technology providers can and should compete based on how their products perform "out-of-the-box." But industry setting the defaults is much different from governments doing so. Given that much of what is filtered, monitored, and blocked to kids is protected speech under the First Amendment, it is not appropriate for governments to decide defaults." – ***Braden Cox, NetChoice***
- "Thoughtful default settings can provide an ease of use for new users, however, since each family's situation and values can differ, settings need to be flexible to meet those needs. If defaults are set, providers should provide clear language about what those settings entail, and clear instructions on how to modify each setting. Defaults that are too restrictive can alienate users by making the Internet experience too cumbersome. For example, if a child is blocked from visiting the majority of the sites he wants to visit, then he'll complain to his parent(s) that the product doesn't "work," and the parent then becomes over burdened with having to manually manipulate settings to allow the child to have a decent experience." – ***Holly Hawkins, AOL***
- "If standardized and adopted across all major media players then more restrictive default settings may have benefits. Standardization of any level of default settings would likely be beneficial as a user would know what information they are displaying or sharing as they move from site to site without delving into their account settings, something the average user is probably not apt to spend a great amount of time doing." – **Hemanshu Nigam, MySpace**
- "Defaults should be set where parents want them. A threshold question about their concerns, values and time to commit to this can help set the right default. Best practice standards will be more effective than governmental nudging or mandates. Default should be set on "non stealth" in monitoring software, and help sites (as brought up by AOL during our session) should not be monitored. (These include child abuse reporting sites, alcohol abuse sites, etc.) – ***Parry Aftab, Wired Safety***
- "You could always force more restrictive settings…that would certainly force folks to get familiar and use the settings but from a provider perspective that is probably a negative on the user experience. This goes to the heart of the Opt In/Opt Out controversy or in other words, mandates or restrictive default settings will be perceived as taking away customers choice, even though they can change them. The better approach is to improve the tools with setup wizards, which at the initial use of the product or service requires the customer to make the choices." – ***Jay Opperman, Comcast***
- "It is not unreasonable to encourage more restrictive default settings given the concerns for protecting children and the likely gap in many parents' technical knowhow. However, parents cannot know if the default sets a parental control option that is more than window dressing. Defaults may create a false sense of security in parents who have no idea what the default means. In addition, teens, who may do most of the computer set up, can easily change the default." – ***Ralph Yarro, Think Atomic***

- "Why not have the default settings be more child protective, and let those who don't want it, opt out? Restrictive default settings will also provide some protection to the novice users." – ***Jeremy Geigle, Arizona Family Council***
- "Instead of pre-set defaults established by the government or technology providers, I think it is better to suggest certain settings for users with an explanation of why the setting is a good choice." – ***Hedda Litwin, NAAG***
- "Restrictive default settings could cause significant consumer backlash and disruption from a use-ability standpoint." – ***Patricia Vance, ESRB***
- "Any governmental mandate of a restrictive default setting would raise serious First Amendment problems, and would very likely be overturned in court. Such a mandate would reduce the flow of lawful information, and would make it harder for content providers on the "restricted" side of the default to reach their audience. Moreover, *any* default setting would be inappropriate for at least some minors – if set for older minors, then it would not protect younger minors, and if set for younger minors then it would infringe on the rights of older minors and those seeking to speak to that audience. A better approach would be to find ways to ensure that users make a choice as to their settings, rather than having the government attempt to make that choice for them." ***John Morris, CDT***
- "This is another area where industry working together could establish best practices and perhaps even some common definitions and settings that would make it easier for consumers and others to use the software 'out of the box.' The Internet changes too quickly for any entity to establish in stone what or how to set defaults. Collaborations between government and industry that includes the consumer voice could prove beneficial to establishing and evolving best practices over time." – ***Michael Kaiser, National Cyber Security Alliance***
- "In extensive conversations with content, platform, and technology providers – and based on the widely diverse composition of Internet users – we are convinced there is no one-size-fits-all solution to this question. A government mandate in this area would be inefficient and ineffective." – ***Rob Stoddard, National Cable & Telecommunications Association***
- "I would caution against the government deciding what defaults are the best – this is very industry and company specific (social networking vs. search, etc). Setting too restrictive default settings can result in a very negative user experience, it is better to teach users about the choices available and how to best use these choices to meet their own needs. If users (children and parents) expect certain defaults they stop being pro-active and really engaging in whether or not that default setting is the best setting for that particular use case." – ***Jill Nissen, Ning***

WHAT IS THE PROPER ROLE FOR GOVERNMENT IN THIS CONTEXT?

Holly Hawkins, AOL:

- Funding for digital media literacy and education programs targeted toward Internet safety and empowering parents and other caregivers to the online risks and tools at their disposal.

- Funding for public awareness campaigns aimed at families focusing the use of safety tools across multiple platforms (cell phones, gaming consoles, computers, etc.) in helping to protect their children.
- Funding for teacher development and curriculum in public schools addressing Internet safety.

Parry Aftab, Wired Safety

- Education, awareness, providing resources to help parents understand options, bringing the industry together, providing guidance on standards.
- Encouraging free products and the industry offering tools that work in tandem with others.
- Testing and making sure that products deliver what they promise.
- Not allowing small print, when companies offer free services and products to mine data from families and kids. Perhaps mandating standard disclosures.

Jay Opperman, Comcast

- Monitor and measure parent satisfaction with product and services and produce hard fact reports
- As a vehicle to facilitate and encourage industry improvement in products and services without mandates
- Provide funding for the education systems to develop the Digital Citizenship training programs and require Parent/Child training to grant online access privileges to under age children in schools and libraries.

Marsali Hancock, iKeepSafe

- Encourage innovation: Tax incentives for voluntary compliance to best practices.
- Provide resources and incentives for professional development for educators, parent education and curricula to be integrated into schools promoting digital citizenship and healthy online use.
- Engage the public health community to develop and implement intervention and prevention strategies for at youth risk.
- Increase resources and training for law enforcement regarding cybercrimes

Jeremy Geigle, Arizona Family Council

- Limited government regulation in the context of protecting children from the harmful effects of the internet.
- Mandated curriculum in the public schools.
- Government incentives given to technology companies (such as tax breaks or rebates) to develop and promote effective internet safety technologies.

Dane Snowden, CTIA

- Education policy and funding.
- Awareness campaigns to ensure parents are taking advantage of available tools and services and children understand how to positively use wireless devices and services.
- Help industry to identify and prioritize specific issues and strike balances between competing interests (i.e. law enforcement v. privacy advocates).

Rob Stoddard, National Cable & Telecommunications Association

- Government oversight of safety, privacy, and security is entirely appropriate.
- Government should also consider supporting and encouraging public/private partnerships to increase awareness of this issue and encourage utilization of marketplace tools. The adoption of a set of national goals for online safety and the designation of a lead agency would be very useful.
- Finally, attention to these issues by local schools, and additional research and work on curriculum development, with proper funding for both, would be helpful.

Ralph Yarro, Think Atomic

"Parents deserve the support of government in making decisions about the education of their children. The laws in place in the real world to protect children largely do not apply online, and where the law does apply, such as the prohibition on obscenity and child porn, enforcement efforts cannot keep up. The Internet is becoming increasingly essential to our children's lives. Parents, industry and the government need to vigorously continue to explore avenues to make children more safe online."

Hemanshu Nigam, MySpace

"In this context all of the pieces are already there and responsible companies have already answered the call to both make their services safer for all users and also to work with third party software providers or technologists when possible. Government would best serve its citizens by then taking the next step in the equation which is educating the public regarding the modern Internet, how their children use it, and most importantly how to engage their children on the subject of responsible Internet use."

John Morris, CDT

"Historically, government mandates in this space have been found to be unconstitutional, except in the narrow circumstance in which a government attaches conditions to discretionary funding. A mandate to require filtering, labeling, or the setting of particular defaults would certainly be overturned in the courts. On the other hand, government support for educational efforts to promote awareness of parental empowerment tools and choices would be both useful and constitutional."

Kevin Rupy, USTelecom

"Government's ideal role in this context is to raise awareness through public awareness campaigns. In addition, Government is ideally suited to support educational efforts aimed at increasing online safety. This can include efforts directed towards educating parents about digital media literacy tools, as well developing public schools curriculum on this issue."

Brian Markwalter, CEA

"[E]ven if we find that parents who are trying to use these tools are generally dissatisfied with them, one cannot conclude that government involvement will help. The companies that make a living selling these tools, online services or devices have the highest motivation to satisfy the parents paying the bills. We need to avoid asking the government to be the nanny, particularly when most parents are not asking for help."

Jill Nissen, Ning

"Government's role should be to provide funding to help educate and raise awareness."

Hedda Litwin, NAAG

"Support and fund a national public awareness campaign."

Michael Kaiser, National Cyber Security Alliance

"Education and awareness presented in a non-biased way that helps parents make informed decisions."

Braden Cox, NetChoice

"Create awareness and education. A few states—including Georgia, Louisiana, and Nevada—have passed laws that requires Internet access providers to make information available to subscribers about products or services that control a child's use of the Internet. In addition, many states now require online education into the classroom curriculum."

WHAT SORT OF ADDITIONAL STUDIES/RESEARCH WOULD BE USEFUL GOING FORWARD? WHAT QUESTIONS DESERVE MORE STUDY?

Holly Hawkins, AOL:

1. How do children of various ages use different types of technology?
2. How do parents want to monitor their child's usage of different types of technology?
3. What types of parental controls do parents use currently and what is the source of the products they use? Do these products meet their needs? If not, what is missing from the equation?

Parry Aftab, Wired Safety

1. What works and what doesn't?
2. What is in the market and what is under development?
3. What do parents want?
4. What do kids want (surprisingly, until they start liking the opposite sex, they are usually fine with parents seeing what they are doing and controlling their access (as long as the innocent sites they want are accessible)?
5. What drive parents to use, abandon or never use these tools?
6. How important is price?
7. Is one product better than several specialized ones?
8. How many households use security suites?
9. What's the current dynamic in the household on parental controls? (Older siblings setting them up, grandparents insisting on their use, etc.)

Marsali Hancock, iKeepSafe

1. New research in the US to correspond to 2009 *EU Kids Online: Final Report* (www.EUKidsOnline.net)
2. Studies around the health, safety, and well being of kids using various types of technology.
3. Studies that reflect the reach and impact and reach of IAD (Internet Addictive Disorder)
4. Studies that demonstrate the effectiveness of various approaches to Internet addiction treatments.
5. Studies to show impact of Web content on other public health concerns, particularly related to self-harm: suicide ideation, anorexia, cutting, etc.
6. Studies that demonstrate the effectiveness of education programs for prevention and intervention for primary risks youth face online (based on EUKidsOnline studies):
    - Reputation: protecting privacy/identity, giving away too much information.
    - Encountering porn
    - Encountering other harmful content (violence, hate speech, self harm information
    - Harassment/encountering unwanted sexual comments.

Hemanshu Nigam, MySpace

"As mentioned earlier there is some fantastic research in this area. In 2008 MySpace helped to form the Internet Safety Technical Task Force whose Final Report was published in December of that year. The research portion of that report demonstrated that there are many, many unanswered questions in this space worthy of research. MySpace endorses the findings of the ISTTF report and its call for future research on the following topics which could help shape policy and understanding of online child safety as a whole: minor-minor solicitation; creation of harmful content by minors; less visible groups such as LGBT youth; the interplay between socioeconomic class and risk factors; the role that pervasive digital image and video capture devices play in minor-to-minor harassment and youth production of problematic content; the intersection of different mobile and Internet-based technologies; and the online activities of registered sex offenders."

Dane Snowden, CTIA

1. *Parental Studies:* Throughout the OSTWG and other working groups, we have seen a number of studies on the ways children use digital technologies and the various affects of those technologies on children. In order to receive a more complete understanding, more research should be done on parental attitudes towards their children's technology use.
    a. What are parental attitudes toward technology? How do these attitudes affect their use of parental empowerment tools?
    b. What concerns parents about their children's technology use? What tools need to be created or modified or are available to address those concerns?
2. *Educational Studies:* How does the U.S. educational system view new technologies? How

can the U.S. educational system best utilize new technologies? (*See U.S. Department of Education, National Education Technology Plan*)

Ralph Yarro, Think Atomic

"A task force study on the effectiveness of different filter option within a controlled environment would be worth doing ("Filter Shootout"). The purpose would not be to promote one filter over another, but to gauge the effectiveness or ineffectiveness of the range of current filter solutions."

Jay Opperman, Comcast

"Long term (over months) ethnographic studies of both parent and child use of controls for younger child and communication techniques between parents and older children."

Rob Stoddard, National Cable & Telecommunications Association

1. Additional research into the effectiveness and utilization of existing parental controls tools – and on prospective features that might improve those tools – would be helpful.
2. And, since parental controls don't exist in a vacuum, research/studies on ways in which online safety controls should be combined with digital media literacy efforts for maximum benefit – in other words extending safety efforts to include "online smarts" – would be helpful.

Hedda Litwin, NAAG

1. Measuring effect of national public awareness campaign in terms of adoption of parental controls.
2. Measuring effect of standardization of controls on usage.

Jeremy Geigle, Arizona Family Council

1. The concept of internet zoning deserves to be debated in the public square and researched further.
2. Research on the mental, social, emotional and physical harms of children accessing inappropriate content.

Braden Cox, NetChoice

"I would like to see more research on how to identify and help at-risk youth. We know from various studies that it is predominantly at-risk youth that seek out inappropriate relationships with adults online, and that meet offline. How can we help these troubled youth?"

Brian Markwalter, CEA

"We should focus, or get the government to focus, on priority risks. Of the top five risks noted in the EU report [2009 *EU Kids Online: Final Report*], the first two (providing too much personal information and encountering pornography), arguably can be helped through default settings and safety tools. The others are not unique to the online world, are not conducive to technology solutions and are complicated by free speech and similar considerations."

John Morris, CDT:

"There are a broad range of potential educational and child safety programs that have been funded in the past, and a broader range of programs that could be funded in the future. With any funding, it is important that the government build in ways to test the effectiveness of the moneys given. In this and other areas of child safety (relating to, for example, drug use and sexual activity) there have been programs that sound good but later prove to be ineffective or counterproductive. We want to promote creative new ideas and approaches, but we should also seek to balance that with assessments of actual effectiveness."

Patricia Vance, ESRB

1. Parental concerns and awareness of online safety risks; what are the real "safety" issues from a parent's standpoint?
2. More nuanced information about the sorts of material/activities that parents want to block or control and how.
3. What are the different risks and preventative measures recommended for different age groups?
4. Behavioral research on *which* factors put *which* kids at risk online.
5. Consumer satisfaction with the tools available today, and why some parents don't use them.

SUBCOMMITTEE ON CHILD PORNOGRAPHY REPORTING

INTRODUCTION

This Subcommittee was charged by the Act "to review and evaluate...

> (2) the status of industry efforts to promote online safety among providers of electronic communications services and remote computing services by reporting apparent child pornography under section 13032 of title 42, United States Code, including any obstacles to such reporting[.]"[53]

The Subcommittee was composed of leading experts on the issue drawn from the private sector, non-profits and academia, with input from governmental agencies. The Subcommittee strove to achieve consensus on the nature of the issues raised by the mandate and the recommendations offered by the Subcommittee. Where members felt that an issue needed further explanation, the Subcommittee provided the opportunity to the individual member to supply an addendum.

The one issue that the Subcommittee immediately encountered was the fact that the statute identified in the mandate was repealed and replaced prior to the convening of the OSTWG. In the PROTECT Our Children Act of 2008[54] – enacted three days later – Congress repealed 42 U.S.C. § 13032, the very reporting provision that OSTWG is charged with studying.[55] Title V of that Act replaced section 13032 with the more detailed service provider reporting procedure for apparent child pornography, along with other related provisions now codified in 18 U.S.C. §§ 2258A through 2258D. The subcommittee felt that it was important to evaluate the replacement statute in a manner consistent with the congressional charge. Therefore, rather than abandon the charter because of the repeal of 42 U.S.C. § 13032, the Subcommittee has undertaken to identify some of the shortcomings of § 13032, compare its reporting provisions to the superseding ones enacted as §§ 2258A and 2258B,[56] and take stock of the effectiveness of the new statute during the brief span of time since its enactment.

OVERVIEW OF SECTION 13032

Originally enacted in 1998[57] as an amendment to the Victims of Child Abuse Act of 1990, § 13032 required providers of an electronic communication service or remote computing service to the public through a facility of interstate or foreign commerce to make a report to a law enforcement agency designated by the Attorney General, as soon as reasonably possible, whenever they obtain knowledge of "facts or circumstances" indicating an apparent violation of enumerated federal statutes relating to child pornography.[58]

The following year, Congress amended that key reporting requirement to direct providers to make their reports, not directly to a law enforcement agency, but instead to the CyberTipline at the National Center for Missing and Exploited Children ("NCMEC"), which was charged with the duty to forward the reports to the appropriate law enforcement agency.[59] Subsequent amendments clarified the responsibilities of NCMEC, authorized it to forward CyberTipline reports to state law enforcement officials,[60] and provided limited immunity for actions taken by NCMEC in the performance of its CyberTipline responsibilities and its efforts to identify child victims.

Section 13032 was an important step forward in clarifying the roles and responsibilities of service providers as involuntary intermediaries in the channels of criminal conduct by which online child pornography is distributed. Reporting apparent child pornography under § 13032 was mandatory for providers – once they obtained knowledge of the relevant facts and circumstances – and failure to report would draw fines of up to $50,000 for an initial failure and up to $100,000 for a second or subsequent failure.[61] Appropriately, however, § 13032 also enacted limited provider immunity, assuring that actions taken in good faith by service providers to comply with the mandatory reporting requirement would not result in civil liability.[62] Perhaps most important for maintaining the proper role of providers, § 13032 made it absolutely clear that nothing in its provisions may be construed by the courts to require providers to engage in monitoring of their users, or of the content of their users' electronic communications.[63]

For all its benefits (including its brevity and simplicity), § 13032 came up short in several respects that became apparent as providers, NCMEC, law enforcement, and prosecutors gained experience with the reporting provisions.

Service providers received little guidance in § 13032 concerning just what "facts or circumstances" relating to the apparent violation of child pornography laws should be contained in the CyberTipline report. The only provision addressing the substance of the report was subsection (d), indicating that a service provider "may include additional information or material" that the provider developed (without describing what that additional information might be), except that "the Federal Government may not require the production of such information or material" in the service provider's report.[64] The vagueness of § 13032 left service providers guessing as to what additional information might be helpful or advisable to provide to law enforcement.

Needless to say, the possession and transmission of images of child pornography are federal felonies. Certainly the providers, NCMEC, law enforcement agencies, and prosecutors all contemplated that the "facts and circumstances" surrounding reportable instances might include the image of child pornography that triggered the reporting obligation. Nothing in § 13032, however, made it explicit that providers would be protected from potential criminal liability for the necessary handling and transfer of such images in the course of their mandatory reporting to NCMEC.

53 15 U.S.C. § 6554(a)(2).

54 P.L. 110-401, Title V ("Securing Adolescents from Online Exploitation"), § 501(a), 122 Stat. 4229 (October 13, 2008). The alternative short title of P.L. 110-401 is the Providing Resources, Officers, and Technology To Eradicate Cyber Threats to Our Children Act of 2008.

55 *Id.*, § 501(b)(1).

56 Section 2258C addresses the potential use of "technical elements" to stop the transmission of child pornography images of identified children – rather than addressing the reporting system itself – and § 2258D relates to limits on liability for NCMEC. Because § 13032 contained no such provisions, the Subcommittee has concluded that examination of §§ 2258C and 2258D lies beyond the scope of the OSTWG mandate.

57 P.L. 105-314, Title VI, § 604(a), 112 Stat. 2974.

58 42 U.S.C. § 13032(b)(1) (1998).

59 P.L. 106-113 Appendix, enacting H.R. 3421 as introduced on November 17, 1999, § 121, 113 Stat. 1535 (codified at 42 U.S.C. § 13032(b)(1) (1999)).

60 P.L. 108-21, Title V, § 508(a), 117 Stat. 683.

61 42 U.S.C. § 13032(b)(3) (1998).

62 42 U.S.C. § 13032(c) (1998).

63 42 U.S.C. § 13032(e) (1998).

64 42 U.S.C. § 13032(d) (1998).

Law enforcement authorities also sought changes to § 13032 that would improve the reporting process and remove unwarranted impediments to investigations of child pornography crimes, such as obtaining readily accessible contact information from service providers, promoting a greater degree of standardization in the content of CyberTipline reports, and permitting NCMEC to forward CyberTipline leads to foreign law enforcement agencies.

The consensus that developed among interested parties seeking improvements in § 13032, as set forth in industry "sound practices" documents[65] and congressional testimony of both NCMEC[66] and service providers,[67] in the context of ongoing dialogue with Members of Congress and their staffs, resulted in the repeal of § 13032 and the enactment of the detailed reporting provisions of Title V of the PROTECT Our Children Act of 2008, codified as 18 U.S.C. §§ 2258A *et seq.*

SUMMARY OF MAJOR REPORTING PROVISIONS OF THE PROTECT OUR CHILDREN ACT

Section 2258A substantially expands and, in contrast to § 13032, makes explicit the range of information that service providers may include in each CyberTipline report. Subsection (a) directs providers to provide detailed contact information in the report, including an individual point of contact, while subsection (b) sets forth five categories of information that providers may include in each CyberTipline report: identifying information concerning the individual who appears to have violated a federal criminal statute relating to child pornography (such as email address, Internet Protocol address, and any self-reported identifying information); information as to when and how a subscriber uploaded, transmitted, or received apparent child pornography, or when and how it was reported to or discovered by the provider; geographic location information, such as a billing address, zip code, or Internet Protocol address; the image of apparent child pornography; and the complete communication containing the image, including data relating to its transmission and other data or files contained in or attached to the communication.

Subsection (c) directs NCMEC to forward each report to the appropriate federal law enforcement agency designated by the Attorney General, and additionally permits NCMEC to forward reports to an appropriate state law enforcement official or, if certain conditions are met, to an appropriate foreign law enforcement agency designated by the Attorney General in accordance with subsection (d). Providers must be notified by NCMEC of the disposition of reports made by the providers as the result of a request by a foreign law enforcement agency.

Subsection (e) increases the fines authorized for knowing and willful failures by providers to make the required report, up to $150,000 for a first failure and up to $300,000 for a second or subsequent failure. Subsection (f), like § 13032, prohibits the courts from construing the statute to require monitoring, either of any user or of the content of any communication of any user, and adds a prohibition against requiring providers to "affirmatively seek facts and circumstances" relating to apparent reportable violations of federal child pornography statutes. Subsection (g) tightly regulates the permissible disclosures of information contained in a CyberTipline report by law enforcement agencies (and by

65 *See, e.g., Proposed Sound Practices for Reporting Apparent Child Pornography*, United States Internet Service Provider Association, http://usispa.org/pdf/US_ISPA_sound_reporting_practices.pdf (visited March 15, 2010).

66 *See* Testimony of Ernie Allen, President & CEO, NCMEC, before the Senate Committee on Commerce, Science and Transportation, Hearing on Online Child Pornography (September 19, 2006), http://www.missingkids.com/missingkids/servlet/NewsEventServlet?LanguageCountry=en_US&PageId=2793 (visited March 15, 2010).

67 *See, e.g.*, Testimony of Elizabeth Banker, Vice President, Associate General Counsel, Yahoo! Inc., before the House Committee on the Judiciary, Hearing on Sex Crimes and the Internet (October 17, 2007), http://judiciary.house.gov/hearings/pdf/Banker071017.pdf (visited March 15, 2010).

providers receiving such information to comply with legal process) or by NCMEC.

Subsection (h) contains an innovative provision intended to assure the prompt preservation of data maintained by service providers that would likely prove useful to law enforcement in investigating leads generated by CyberTipline reports. It requires providers to treat NCMEC's notification of receipt of a CyberTipline report as a request to preserve subscriber information under 18 U.S.C. § 2703(f), a well-established procedure that law enforcement routinely employs to prevent the deletion or overriding of data in a subscriber's account pending issuance of legal process to compel production of the data to investigative authorities. The new provision requires service providers to preserve the contents of the CyberTipline report and any images or files commingled or interspersed among the images of apparent child pornography within a particular electronic communication or user-created folder or directory, and to limit access to preserved data (which is likely to include material that is otherwise illegal to possess).

Section 2258B provides immunities for the entities involved in the reporting system set out in § 2258A. Section 2258B elaborates upon the immunity provision of § 13032 to bar not only civil claims but also criminal charges against service providers, domain name registrars, or their officers and employees arising from performing their duties under the new statute, unless they engaged in intentional misconduct or acted recklessly or with actual malice or for a purpose unrelated to their duty to report or preserve data. It also requires providers and registrars to minimize the number of employees who have access to images and to permanently destroy any images at the request of law enforcement.

RECOMMENDATIONS OF THE SUBCOMMITTEE

The Subcommittee notes that the reporting statute which it is our responsibility to analyze, 42 U.S.C. § 13032, by examining industry efforts to promote online safety and any obstacles to effective reporting under that statute, is no longer in effect, having been superseded in October 2008 by the provisions of 18 U.S.C. §§ 2258A *et seq.*, enacted as part of the PROTECT Our Children Act of 2008.

Having heard from a variety of experts and received presentations on a range of issues during Subcommittee meetings, it is clear that the new reporting and expedited data preservation procedures in the PROTECT Our Children Act have resolved a number of concerns expressed by providers, the law enforcement community, and NCMEC over the limitations of § 13032. In particular, two features of the new reporting and data preservation provisions of the Act were cited favorably by panelists addressing the Subcommittee.

First, as required in § 2258A(h)(3), having service providers preserve any images, data, or files commingled with the image that generated the CyberTipline report, for later disclosure to law enforcement, is likely to yield crucial evidence to investigate and prosecute offenders and successfully identify child victims. Second, having service providers forward to the CyberTipline the complete communication containing the reported image, any other images or files, and related transmission data, as called for in § 2258A(b)(5), will likely also bring to light other important investigative leads and enable the identification of child victims.

The Act appears already to have had a significant impact on the volume of CyberTipline reports made to NCMEC by service providers. NCMEC's overview of the operation of its CyberTipline, included as an Addendum to the Subcommittee report, shows that the number of CyberTipline reports received from service providers increased 84% from 2008 to 2009, the first full year the new reporting and data preservation provisions in the Act were in effect. There were 33,160 reports by providers to the

CyberTipline in 2008, and 61,055 in 2009. For the first quarter of 2010, the number of CyberTipline reports from providers totaled 27,144, on pace for another remarkable year-to-year increase of 78% from 2009 to 2010. Notably, the 2009 and 2010 CyberTipline reports include the additional images, data and other files called for in the PROTECT Our Children Act to facilitate criminal investigations of child pornography offenses and the identification of child victims. The number of images and videos reported by service providers totaled 609,206 in 2008, 700,939 in 2009, and 390,393 – for the first quarter alone – in 2010.

Overall, there has been a substantial increase in these numbers since the reporting and data preservation provisions of the Act have taken effect, which the Subcommittee hopes will accelerate investigative efforts and spur additional criminal prosecutions of child pornography offenders.

1. *Congressional commission of a survey of providers*

Regarding industry efforts to promote online safety in connection with the new reporting and data preservation regime enacted in the PROTECT Our Children Act, the Subcommittee's attempts to gather information have been only partially successful. The preferred approach to fact-finding on this issue, conducting a survey of providers of electronic communications services and remote computing services with the prior approval of the Office of Management and Budget under the Paperwork Reduction Act,[68] could not be accomplished within the time frames and resources available to the Subcommittee.

The Subcommittee recommends, therefore, that Congress task the appropriate executive agency with the objective to conduct a survey, using an empirically reliable methodology, to assess industry efforts to promote online safety by means of the new reporting provisions of § 2258A.

2. *Education and outreach to providers and law enforcement*

As noted above, the major providers of electronic communications service and remote computing service have not only been publicly supportive of the provisions of the PROTECT Our Children Act, but in fact conceived and promoted some of the original legislative proposals embodied in the Act.[69] Members of the Subcommittee expressed concern, however, that service providers at the regional and local levels, as well as some federal, state and local law enforcement agencies, may not yet be completely familiar with the new reporting provisions and data preservation procedures established in the Act. Ensuring that law enforcement officials and service providers at all levels are fully informed about all aspects of the Act will promote increased reporting, more effective investigations, and a greater number of successful prosecutions.

Subcommittee members have noted that newly established companies and smaller providers who lack in-house expertise on child online safety issues may be unaware of what to do when they encounter images of child pornography for the first time, and putting the appropriate processes in place for reporting and preservation can be daunting. Subcommittee member Parry Aftab has submitted a separate statement (included as an Addendum to this report) setting forth the challenges entailed in developing and deploying procedures to report child pornography to the CyberTipline in an efficient, safe and secure manner.

NCMEC is already helping to overcome these obstacles by engaging in extensive outreach efforts to service providers to apprise them of the reporting requirements and data preservation procedures in the Act. Providers in start-up mode or those who have not availed themselves of the advice of legal counsel or other expert advisors are especially likely to benefit from NCMEC's efforts.

To cite just one example of NCMEC's outreach, service providers that submit reports manually may not be aware of significant cost savings that might be possible by automating the reporting process. To assist companies with automated reporting into the CyberTipline, NCMEC has created a document detailing the interface for its CyberTipline application to enable service providers to submit reports in "batch mode," a method of volume reporting that requires minimal human intervention.[70,71]

The Subcommittee therefore recommends that NCMEC, government agencies, advocacy groups, and service providers continue to undertake education and information-sharing efforts to promote awareness of the PROTECT Our Children Act, particularly those provisions that widen the scope of information included in CyberTipline reports and expedite the preservation of provider data related to the transmission of images of apparent child pornography. Service providers with extensive prior reporting experience under § 2258A and its predecessor statute can assist in this effort by distributing sound practice guidelines for the benefit of providers that are just beginning to design and develop their own reporting and preservation procedures.

3. *Meetings among service providers, NCMEC, and law enforcement*

Subcommittee members who work closely with service providers emphasized that maintaining an ongoing dialogue with NCMEC and law enforcement can significantly improve providers' understanding and execution of child safety initiatives as well as performance of their reporting obligations. Too often, however, start-up companies and smaller providers fail to proactively seek out meetings with NCMEC and law enforcement, for a variety of reasons ranging from lack of acquaintance with the appropriate personnel to fear of unspecified consequences of direct engagement with law enforcement.

The Subcommittee therefore recommends that service providers, particularly those that are in the initial phase of designing processes to report apparent child pornography violations, meet with NCMEC and law enforcement agencies to broaden their practical understanding of compliance issues and help them more efficiently perform their reporting and preservation obligations under the Act.

4. *Technology and information sharing among service providers*

The Subcommittee noted the impressive collaboration that service providers and other participants in the information technology industry have undertaken for years, through joint endeavors such as NCMEC's partnership with the Internet industry consortium known as the Technology Coalition[72] and others. Through these efforts, service providers have developed and deployed innovative technological solutions that disrupt the transfer of online child pornography and facilitate reporting to

68 44 U.S.C. §§ 3501-3520.

69 *See* text accompanying notes 14-16, supra.

70 *National Center for Missing and Exploited Children CyberTipline II Interface* (document available from NCMEC). NCMEC has designated its service provider reporting facility as "CyberTipline II" to distinguish it from the facility for reporting by the public, "CyberTipline I."

71 As Subcommittee members noted, there may be significant up-front costs to implement automation before any cost savings can be realized.

72 See "Online Industry Leaders Announce New Effort to Use Advanced Technologies to Help Combat Child Exploitation" (publicizing formation of the Technology Coalition), NCMEC Press Release (June 27, 2006) http://www.missingkids.com/missingkids/servlet/NewsEventServlet?LanguageCountry=en_US&PageId=2442 (visited March 16, 2010).

NCMEC.[73]

The Subcommittee commends these efforts and encourages continued cooperation among industry participants. Service providers should continue their endeavors to share technologies that can support leading-edge reporting tools for use across diverse networks and platforms, in order to reduce reporting costs for all providers.

5. Incentives to assist providers with new data preservation and security mandates

One of the key new requirements of the PROTECT Our Children Act (described above in the summary) calls for service providers to preserve a range of images, data, and other digital files when they receive NCMEC's notification of receipt of a CyberTipline report. Subsection (h) of § 2258A instructs service providers to treat the notification as a request to preserve subscriber records under 18 U.S.C. § 2703(f), including the CyberTipline report itself (which in most cases will contain an image of apparent child pornography), together with any images, data, or other digital files commingled or interspersed among the images of apparent child pornography within a particular communication or user-created folder or directory. Gathering and segregating this data can be time-consuming and labor-intensive, particularly for providers offering high data storage capacity at low (or no) cost to users, and storing it entails additional expense for which providers have no reimbursement mechanism.

In addition, because it would be unlawful, in any other context, for private entities to store these materials, Congress imposed requirements that providers develop security measures to protect against disclosure, including maintaining the preserved files and data in a secure location, minimizing the number of employees that are provided access to images, and restricting access by agents or employees to only to what is necessary to comply with the preservation requirements. These preservation and security mandates, which are entirely appropriate and justified, nonetheless go well beyond the predecessor statute's requirement to report apparent child pornography violations. Security for ultra-sensitive data, together with access and minimization requirements, establish real infrastructure costs to be borne by providers, costs that are rapidly increasing in magnitude with the surge in the number of images of apparent child pornography reported to the CyberTipline by providers (on track to exceed 1.5 million in 2010 alone).

The Subcommittee therefore recommends that Congress consider tax credits or other financial incentives to assist service providers to bear the development and implementation costs of the preservation and security requirements established in the PROTECT Our Children Act.

6. Incentives to establish wellness programs for compliance staff

Finally, the Subcommittee took note of the emotional toll incurred by employees who face the task of reviewing abhorrent images of child sexual abuse in the course of their job responsibilities to fulfill their employer's compliance obligations with Congress's mandatory child pornography reporting requirements. Congress should consider providing incentives and other assistance to service providers for the specific purpose of helping establish wellness programs and other beneficial measures to address the psychological impact on employees of exposure to these disturbing images.

Separate Statements of Subcommittee Members Included as Addenda

Subcommittee member Parry Aftab of WiredSafety has provided a separate statement identifying some of the costs she believes service providers incur in reporting online child pornography under the provisions of § 13032 and the successor provisions of §§ 2258A and 2258B. These costs encompass the technology, programming, and human resources necessary for (1) the initial review and reporting of images, (2) the required data preservation and storage called for in the PROTECT Our Children Act, and (3) the timely and complete compliance with legal process served by law enforcement agencies associated with reports made to the NCMEC CyberTipline. Accordingly, she expands upon the Subcommittee's recommendations relating to data preservation and security by calling upon Congress to consider additional financial incentives to help service providers put into place technologies for efficient, comprehensive, and automated reporting to NCMEC and to assist providers in hiring and retaining reporting and compliance staff. Her statement also sets forth issues for further consideration by Congress, service providers, law enforcement, and advocacy groups, including (among others) how service providers should handle "sexting,"[74] whether safe harbors based on industry sound practices would be a useful adjunct to the immunities granted under the PROTECT Our Children Act, and legal concerns arising from exposure to child pornography by providers' compliance staff.

Subcommittee member John Shehan of NCMEC provides an overview of the operation of NCMEC's CyberTipline, including statistics on reporting by members of the public as well as service providers for the period from 1998 through the first calendar quarter of 2010.

Subcommittee member John Morris of the Center for Democracy and Technology details a series of proposed factual inquiries that they believe Congress should undertake in order to evaluate how the expanded reporting system forged by the Act has affected the initiation of criminal investigations as well as the course of prosecutions in child pornography cases. Without a more complete picture of the law enforcement processes and outcomes, Congress may be hampered in its decision-making on how to allocate funding and direct oversight of the overall effort to fight child pornography.

Inclusion of Subcommittee members' separate statements provides a more comprehensive view of the concerns considered by the Subcommittee but does not represent endorsement of any additional recommedations by the Subcommittee as a whole.

CHILD PORNOGRAPHY REPORTING SUBCOMMITTEE: ADDENDUM A

STATEMENT OF JOHN MORRIS OF THE CENTER FOR DEMOCRACY AND TECHNOLOGY

Questions for Further Study

73 See "Microsoft and National Center for Missing & Exploited Children Push for Action to Fight Child Pornography" (announcing PhotoDNA technology to enhance detection of known images of child pornography), NCMEC Press Release (December 15, 2009) http://www.missingkids.com/missingkids/servlet/NewsEventServlet?LanguageCountry=en_US&PageId=4168 (visited March 16, 2010).

74 "Sexting" in this context refers to the creation, sharing and forwarding of sexually suggestive nude or nearly nude images by minor teenagers, usually but not exclusively on mobile devices. See Amanda Lenhart, Teens and Sexting (Pew Internet & American Life Project, 2009) http://www.pewinternet.org/Reports/2009/Teens-and-Sexting.aspx (visited April 21, 2010). Subcommittee members discussed sexting where the content includes photographs or videos that might meet the statutory definition of child pornography under 18 U.S.C. § 2256(8).

Congress directed OSTWG to evaluate the "status of industry efforts to promote online safety" through the statutorily mandated system of reporting apparent child pornography to NCMEC, and we have in this report attempted to meet that mandate. It is important to note, however, that to fully evaluate the impact of the reporting system, it is vital that Congress also evaluate the status of the investigative and prosecutorial efforts into which the reporting system flows. Without knowing how the reports are processed and handled through investigation and prosecution, it is impossible to know whether the reporting system is making a significant impact.

To illustrate this concern, the changes to the reporting system (from 47 U.S.C. § 13032 to 18 U.S.C. § 2258A) were presumably made in part to increase the level of reporting of apparent child pornography. Yet without knowing whether the investigative and prosecutorial agencies have the resources to pursue an increased number of reported cases, it is very difficult to evaluate how much impact the changes in the reporting system are actually having. And most critically, without a complete picture of the entire effort to fight child pornography, Congress cannot appropriately determine how to allocate funding or direct oversight.

To evaluate the complete picture, it would be important to collect and analyze a thorough range of data, including at least the data points listed below. A few of the data points are available, and OSTWG heard reports touching on some of the data points, but most are not available in any public form. The important data points include:

- The number of complete reports[75] of apparent child pornography received by NCMEC for relevant reporting periods (such as per month and per year), broken down by the online communications method involved (*e.g.*, websites, e-mail, etc.).
- The number of images of apparent child pornography referenced in those reports.
- The number of *unique* images referenced in those reports.
- For websites, the number of unique websites referenced, and the number of unique domains referenced.[76]
- Of reports received by NCMEC, the breakdown between emergency or expedited reports (addressing real time threats to minors) and standard reports.
- Of reports received by NCMEC, the breakdown between reports for which NCMEC determined that apparent child pornography was present, and reports where a different conclusion was reached.
- The average time NCMEC takes to process and review the expedited and standard reports, from the time received until the time a report is closed or transmitted to law enforcement.[77]
- For reports transmitted to law enforcement, a breakdown of what agencies received the reports.

75 Because of the mechanics of the online reporting system, OSTWG was told that service providers at times had to break an individual report into multiple submissions using the online system.

76 It is important that Congress receive details of the reports rather than aggregate numbers. One child pornography reporting hotline recently released preliminary information indication that out of 80,000 reports of apparent child pornography, more than 50,000 reports were duplicates (reporting the same web content, for example), and the non-duplicate reports ultimately pointed to about 600 unique websites. See Stephen Yagielowicz, "ASACP Preparing CP Reporting Hotline White Paper" (Mar. 25, 2010), available at http://www.xbiz.com/news/118917. To properly determine how best to deploy investigative funding and attention, it is vital that Congress receive and understand both the aggregate numbers (like 80,000) and the detailed numbers (such as 600).

77 To be clear, by suggesting these questions, we in no way wish to suggest a concern that NCMEC does not process the reports very promptly. Based on the evidence we heard, NCMEC appears to act with appropriate efficiency.

- For the Department of Justice and other law enforcement agencies receiving reports from NCMEC, the average time from the time of the NCMEC transmittal until (a) an initial review of the content involved was completed, and (b) formal investigative steps were undertaken.
- For the Department of Justice and other law enforcement agencies receiving reports from NCMEC, a breakdown of how many NCMEC reports (a) were pursued with an active initial investigation, (b) were not pursued because of resource constraints, (c) were not pursued because the agency did not think the content included apparent child pornography, or (d) were not pursued because of another reason.
- For the Department of Justice and other law enforcement agencies receiving reports from NCMEC, with regard to reports leading to an active initial investigation, a breakdown of how many investigations were later dropped because of resource constraints, evidentiary gaps, or other reasons, and an indication of the dispositions of the investigations that did proceed.

Only by following through to the end of the prosecutorial process can Congress fully assess the impact of the child pornography reporting system. The above facts (and certainly others that we have not identified) can provide a fuller picture of the value of the reporting system. Pursuant to Section 502(b) of the PROTECT Our Children Act, the General Accountability Office is currently conducting an evaluation of some (or all) aspects of the child pornography investigation process, with a report to Congress due four or more months after this report. We urge the GAO to consider the questions raised here in its research and report.

CHILD PORNOGRAPHY REPORTING SUBCOMMITTEE: ADDENDUM B

NATIONAL CENTER FOR MISSING & EXPLOITED CHILDREN (NCMEC): CYBERTIPLINE

18 U.S.C. § 2258A and its predecessor 42 U.S.C. § 13032 require electronic service providers (ESPs) to submit reports regarding apparent child pornography to the NCMEC CyberTipline.

Authorized by Congress and launched in March of 1998, the CyberTipline offers a means of reporting incidents of child sexual exploitation including the possession, manufacture, and/or distribution of child pornography; online enticement; child prostitution; child sex tourism; extra- familial child sexual molestation; unsolicited obscene material sent to a child; and misleading domain names, words, or digital images. The CyberTipline is staffed 24 hours a day, 7 days a week.

ESPs have submitted 44% of all CyberTipline reports received. Through the ESP reporting process, more than 6.5 million suspected child pornography image/videos have been removed from the

Internet and reported to the CyberTipline along with details of the incident.

Year	Number of Images/ Videos submitted by ESPs
1998	0
1999	0
2000	0
2001	421
2002	17,866
2003	324,166
2004	1,152,944
2005	501,587
2006	1,043,144
2007	1,830,961
2008	609,206
2009	700,939
2010*	390,393
Totals	**6,571,627**

*2010 1st Quarter only

Year	Number of CyberTipline Reports from the Public	Number of CyberTipline Reports from ESPs	Total number of CyberTipline Reports Received
1998	4,560	0	4,560
1999	9,668	0	9,668
2000	19,245	0	19,245
2001	23,482	960	24,442
2002	33,744	9,334	43,078
2003	33,857	48,102	81,959
2004	33,697	78,320	112,017
2005	39,112	31,656	70,768
2006	44,419	32,165	76,584
2007	69,414	35,847	105,261
2008	68,869	33,160	102,029
2009	58,492	61,055	119,547
2010*	17,875	27,144	45,019
Totals	**456,434**	**357,743**	**814,177**

*2010 1st Quarter only

Any incidents reported to the CyberTipline online or by telephone go through this three-step process.

- CyberTipline operators review and prioritize each lead.
- NCMEC's Exploited Children Division analyzes tips and conducts additional research.
- All information is accessible to the FBI, ICE, and the USPIS via a secure Web connection.

Information is also forwarded to the ICACs and pertinent international, state, and local authorities and, when appropriate, to the Electronic Service Provider.

NCMEC's CyberTipline is operated in partnership with the Federal Bureau of Investigation (FBI), the Department of Homeland Security's Immigration and Customs Enforcement (ICE), the U.S. Postal Inspection Service (USPIS), the Internet Crimes Against Children Task Forces (ICACs), the U.S. Secret Service (USSS), the U.S. Department of Justice's Child Exploitation and Obscenity Section (CEOS), as well as other international, state, and local law enforcement.

CHILD PORNOGRAPHY REPORTING SUBCOMMITTEE: ADDENDUM C

THE REALITIES AND OBSTACLES OF CHILD PORNOGRAPHY REPORTING FROM THE TRENCHES

By Parry Aftab, Esq., WiredSafety.org

I have practiced Internet compliance and privacy law since 1994, and have advised many industry leaders and smaller companies in child pornography reporting. Over the years, I have learned that a day-in-the-life of a service provider, social network or game network is challenging. They deal with codes, users and try to figure out the laws and best practices as best they can. Understanding their challenges will help us address child pornography reporting deficiencies better and more efficiently. This addendum is appended to the subcommittee's report (to which I contributed as a member of the OSTWG and of the subcommittee) to point out some practical implications of the child pornography reporting law. While there are ways to address and remedy these practicalities, as set forth in the entire sub-committee's report, it might be helpful to understand them from a provider's perspective.

First we should understand that providers come in all sizes, styles and levels of experience. There is no one-size-fits-all when providers are involved. Some are well-established large multi-national corporations, such as Facebook, MySpace, AOL and Microsoft. Others are either small and will stay that way, start-ups that can go in either direction or companies with new products and services that are just being developed and not well understood. Obviously the large multi-national entities have layers of risk management staff and may have someone assigned fulltime to handling child pornography and the requisite reporting and compliance issues. Others use one or more in-house lawyers or paralegals to handle these responsibilities. In some cases the head of customer service, or the company's in-house policies and abuse or moderation team is in charge of high-risk issues, including child-pornography handling and reporting. A few may assign this to their security or IT teams. And, in the case of some start-ups, even well-funded ones, they are not aware that they have a legal obligation to do anything once they discover child pornography and wouldn't know what to do even if they were aware of the law.

Notwithstanding the famous success stories of Facebook and MySpace, where start-ups quickly

become large multi-national entities and can afford trained and talented professionals to advise them on risk management, or smaller start-ups like Ning and Twitter that despite the companies' size (fewer than 200 employees) and without the same financial resources of larger companies, have devoted significant resources into legal compliance and developing best practices, the reality of being a provider these days is challenging. Personnel and IT come at a premium. Venture capitalists, banks and other common sources of funding are harder to source. Expected capital infusions no longer arrive on target. Some companies are located in out-of-the-way places and have difficulty finding local trained professionals or those willing to relocate. The competitive situation is stiff. Users of all ages are expecting online services to be provided without charge and are resisting many paid sites, networks and services. This puts further pressure on the business to cut costs and corners. While they care about doing it right and about the safety and welfare of children, they quite simply may not be able to afford to care. If it's between meeting payroll, finishing a game build or securing your data and staffing and designing a child-pornography compliance system, their continued survival might compel them to wait a bit longer to do nothing more than the bare minimum to comply with the law. As we heard from Ning, a start-up that made the decision to invest the time, money and resources not to just simply comply with the mandatory reporting requirements under §§ 2258A, but to be pioneers for a company their size in developing back-end tools that would allow them to safely, efficiently and securely provide much of the additional information that is now suggested in §§ 2258A(b) – including the actual images of apparent child pornography – doing so was extremely costly and would likely be prohibitive to many.

It's ironic that technology providers may be challenged by technology, but it's a reality. Privacy, safety and security professionals understand that products, services and systems must be designed with these risks in mind. Many large and now successful entities are still working with technologies held together "with bubble gum, chicken wire and toothpicks," as the head of IT of a social network informed me a few years ago. They are often so busy trying to manage the growth, they don't have time or the resources to manage the risks. They stick their thumbs into the dike hoping it will hold when they find new risks. They fully intend to come back and fix these problems, but often don't have the time or resources to do so, or forget that they ever existed until they arise again. Some technologies are so new that collection, storage and evidencing data is unresolved. They know they work for gaming or community interactions, but don't fully understand evidence collection and the ability to generate data reports surrounding child pornography.

And when a system is fully designed and already operating, compliance is difficult to implement. The developers and technology designers need to be informed about the compliance needs at inception. They need to understand these things *before* they code, not learn about them afterwards. Finally, who is going to pay for this and how? What are the hard and the soft costs? Do their top programmers need to be diverted from profitable builds to these "money pits"? What's the least they can get away with? There is a good deal of confusion about child pornography and what the providers are expected to do to comply. Laws change and, when they do, the whole risk management process begins anew. What had been cobbled together to comply with the previous law now needs to be re-examined by professionals to see if it must be revised or scrapped to comply with the new one. Some aren't sure they know where the "child being bathed" ends and the "child pornography" begins. Many users who report images are confused as well. While many images clearly constitute child pornography, many others fall into a legitimate grey area, or a grey area that is purely created by the provider's lack of understanding.

What about the recent rise in "sexting" where teens and preteens take, share and possess sexual images of each other? ("Sexting" combines "sex" and "texting" to reflect that a vast majority of

"sexts" are taken and transmitted using cell phones and texting devices. But sexting is not limited to handheld devices. Webcams built into most desktop gaming devices, handheld gaming devices and laptop computers, as well as those that are added to the desktop computers, are often used by teens or preteens to transmit their sexual videos to other teens or preteens (and sometimes adults). These images, although they don't fall into what had previously been thought of as "child pornography" still constitute "child pornography." MTV and the Associated Press polled teens and learned that about a third of them had sent or received a sext. They may have sent it to or received it from their boyfriend or girlfriend on a one-to-one basis, or from bullies who forward sexting images they encounter. Sometimes disgruntled ex-friends broadcast previously private images.

Questions that arise in the provider space: How does the reporting process work? And how are providers supposed to develop a faster and more efficient system for gathering the requisite information and handling the images in a legally-compliant manner? If they become aware of one image within a particular group or page, should they search through the entire group or page where the image was located to find others, even if not required to? What if they report an image and they are wrong? What if they turn over information about their users and they are wrong? What are they required to do and what is purely elective? These questions need to be answered clearly and easily if the system will be adopted across all US providers.

What are the legal implications to the provider for complying or failing to comply? It's one thing to say that there are severe penalties for non-compliance, but what about existing privacy policies that promise users that their information will not be shared with third parties other than "as may be required by court order, warrant or valid subpoena" or similarly defined law enforcement and legal compliance language? Providers may find themselves between the rock of their privacy policy and liability for violating its terms and the hard place of child pornography reporting legal compliance. Changing their privacy policy to give them the authority to turn over information "in compliance with applicable law," or "to protect the safety and security of its users, the public at large or its network" may work for prospective users and data collected following the effective date of such a revised policy, or for users who "accept" any retroactive terms by continued use or opt-in mechanisms, but won't work for anyone else. Is there a safe harbor for their complying by providing information collected under terms that prohibit its use?

What about overall risk management issues, such as human resources, security and insurance? Can they become liable for workplace safety and wellness claims resulting from emotional trauma and stress-related health issues experienced by employees responsible for reviewing the child pornography images, handling the evidence gathering or making the reports? What if their moderation teams are outsourced offshore? Should the contracts include special provisions waiving claims by the outsourced personnel responsible for this task or who may come into contact with child pornography before forwarding it on? How can they be certain that what works in the US doesn't conflict with Philippine, Canadian, Indian, Pakistani or Irish laws? Is transmitting those images across country borders illegal? If so, as many would conclude, there are additional costs involved in developing additional back-end tools and systems to allow outsourced contractors to only access that portion of the a company's servers where the child pornography is securely stored. How can they secure the images and information offshore and be confident that they have taken all necessary steps? What happens if an employee of the company misuses the images or information? What about insurance? Are there special policies they should be buying or riders they should be seeking? Do their security practices need to change? Do they have to apply encryption to the images and data they are collecting? Who legally can and who should have access to that information? How do you permanently delete illegal images once turned over or moved to special evidence storage servers?

What steps should be taken to secure the evidentiary value of the information they have on file? What works for others? Are there groups they can join to help them tackle this better? Are there financial barriers to entry to these groups for smaller companies? Are there trustworthy advisors they can afford? Is there language that they should be adopting as part of their privacy policy, terms of use or codes of conduct? If so, where can they find it? What technologies or practices have worked for others, and how much do they cost to purchase, develop or implement? Are there training programs available or professionals to help advise them? Are there watchdog groups that report non-compliers? Are there benefits, other than legal compliance itself, for complying with the law? What happens if they make a mistake and under- or over-report images?

Most industry members, large and small, established and start-up, want to comply. They care about the issues, and are often parents as well as business people. But until we can make this easier for them, and make sure their questions are answered and their confusion addressed, the laws designed to make children safer will not be as effective as they can and should be.

SUBCOMMITTEE ON DATA RETENTION

The Congressional mandate creating the Online Safety and Technology Working Group (OSTWG) called for the committee to...

> *"evaluate the practices of electronic communications service providers and remote computing service providers related to record retention in connection with crimes against children."*

Accordingly, a subcommittee was formed to examine the practices of law enforcement, Internet Service Providers, and content and application providers concerning the retention of data that may be requested by law enforcement when investigating crimes against children. Unlike some of the other areas examined by OSTWG, there is not – either within OSTWG or the broader community – consensus on whether any data retention mandates should be imposed on service providers.

Data retention is a very contentious subject from a policy perspective. In the U.S., competing interests include those of law enforcement as they investigate crimes against children carried out or facilitated over the Internet, the Internet industry that retains certain data (primarily for business reasons), and the end-users who have privacy concerns. Consequently, this section of the report provides the three pertinent perspectives on this subject: law enforcement, industry, and consumer privacy. Ultimately, when talking about data retention we must strive to achieve the right balance between often competing and conflicting requirements.

FINDINGS

HISTORY OF DATA RETENTION

The business practice of retaining certain data related to telephone calls originated in the earliest days of telephony. Because tariffs differed region by region, or even state by state, detailed records had to be kept for each call principally so that the proper billing rate could be applied to each call and the customer billed appropriately.[78], [79] These "call detail records" contain at least the following information: the calling number, called number, the date and time of the call, call duration, and other information to facilitate bill reconciliation.

When cable system operators began to enter the telephony business in the 1990s, they began retaining data records on telephone calls made by their subscribers for similar business reasons.

Because customers sometimes disputed their bills, call detail records were kept for a few months, and then destroyed when there was no longer a business purpose for them to be retained by the service provider.

78 Since 1986 the Federal Communications Commission (FCC) has ordered the retention of telephone toll records by commercial carriers. See 47 C.F.R. §42.6. At a time when telephone service was the only real-time means of communication and when non-toll, local telephone service was largely limited to the immediate vicinity of a town or municipality, these regulations effectively require the retention for eighteen (18) months of "destination" information (i.e., "telephone number called") for every telephone call of any significant distance.

79 Not only is there an FCC requirement to retain telephony call detail records but each state has record retention requirements, principally through their state PUC. Some require that subscriber information or copies of bills be held for a handful of years.

Law enforcement and private litigants soon recognized that these call record databases contained information that could facilitate investigations and litigation. Because the telephone companies could match a telephone number in a call detail record with a subscriber's street address, both the criminal and civil justice systems began to use compulsory process to obtain these records. These records play an important part in our nation's system of criminal and civil justice because they typically represent accurate, objective, and relevant evidence generated by an otherwise disinterested third party (i.e., the provider), thereby minimizing reliance solely upon witness memory and testimony. Today, such business records continue to be used routinely by both the prosecution and defense in criminal cases, including cases involving the abuse of children.

DATA RETENTION PRACTICES TODAY

The mid-1990s saw the emergence of broad, popular use of the Internet and the "World Wide Web," as millions of users began to send email and exchange information (including still images and, recently, videos) with each other over this new communications medium. In the early days most users accessed the Internet through phone lines. Thus, phone companies could often still provide law enforcement with call detail records showing when a user dialed an Internet access number, how long they stayed connected, and what access number they dialed (but not online information such as where a user went on the Internet). For example, law enforcement could find out a subscriber dialed into his AOL account at 10 PM and stayed logged in for 2 hours by obtaining call detail records from that subscriber's phone company, but they could not determine from the telephone records what sites were visited, what messages he might have sent (or to whom), or whether he was even actually at his keyboard for the entire time he was logged in.

As more users moved to "always-on" broadband connections (using, for example, cable modem, DSL or fiber optic technology), telephone and cable telephony call detail records were of little or no use, since broadband service did not rely on telephone company switching equipment to maintain their connections. However, like their telephone predecessors, Internet Service Providers (ISPs) also need to keep track of each account in order to resolve any billing disputes, or to troubleshoot connections in the event of a failure. Once again, records kept by cable and telephone companies proved useful to law enforcement and private litigants to gather evidence for criminal or civil proceedings.

The records are generated as soon as a person connects to the Internet. Whenever a computer or home router initiates a connection over a common residential broadband access network, one of the first things that happens is that it is assigned a unique IP address by the ISP to which the household subscribes. When the user then posts a file on a website or sends an email, the IP address of the computer or home router and the date and time when those electronic communications occur may sometimes be captured. Since ISPs control only certain ranges of IP addresses, a given IP address can be traced to the ISP which assigned it. Knowing the IP address and date and time an activity occurred, the ISP can identify which subscriber was assigned that IP address at the relevant date and time. This data, which enables law enforcement to trace back from the scene of an Internet crime to find the account used to commit that crime, is part of what is often referred to as "source data," and is described more fully below.

Records from ISPs differ somewhat from telephone call records in several key aspects:

1. Internet Protocol (IP) addresses, which may identify unique computers on the Internet, are somewhat analogous to telephone numbers, but with some important differences. Phone numbers are "static," meaning the same number will usually be assigned to the same subscriber so long as the user maintains the account. In contrast, for residential broadband connections, IP addresses are usually "dynamic," meaning that a given IP address will only be temporarily assigned to a user. A dynamic IP address is usually assigned to a user either just for a single session of Internet access, or for a brief period of days or weeks, after which, if the subscriber continues to access the Internet, the subscriber could be assigned a different IP address. Unused IP addresses are recycled back into a "pool" of addresses and can be re-assigned as needed to different subscribers. (Occasionally, however, IP addresses are "static" in that an ISP assigns one IP address to a subscriber on a long-term basis.[80])
2. An ISP generally has no knowledge of where on the Internet their subscriber has visited; all the ISP usually knows is that their subscriber was assigned a particular IP address (for example, 170.110.225.163) from time A to time B. But, unlike telephone call detail records (which are used for billing the customer), an ISP historically has had little (if any) business reason to retain information on IP address assignments.
3. IP addresses can be spoofed, i.e., someone can make their computer appear to be using an IP address that actually belongs to another user, thus making it nearly impossible to match the IP address with the right user's street address. In contrast, because telephones were generally "hard-wired" to a physical street address, spoofing of phone numbers was historically much less likely (although today, Caller-ID spoofing is possible).
4. Although possible, it is not easy for an individual to use someone else's phone service without the account holder's permission. In contrast, in cases where a broadband subscriber allows wireless Internet access without requiring a password, it can sometimes be easy for an unauthorized person to access the Internet connection. For example, someone can park nearby and connect to the Internet through a subscriber's unsecured home wireless network[81], and through that connection access any Internet content (including, possibly, illegal or pirated content).

Despite these differences, Internet records have proven to be useful to the criminal and civil justice systems.

However, there are financial and legal pressures on companies not to retain data for long periods of time. With ISPs, once a subscriber has paid their Internet access bill, there may be no incentive for an ISP to keep the record – disk storage, while relatively cheap, is still expensive when terabytes of storage are involved, over and above the costs of securing and retrieving data records from some storage archive. As for legal pressures, federal privacy and state data breach notification laws may apply to "personally identifiable information" retained by a telephony or Internet access provider, thus giving the provider an incentive to retain that information for the shortest amount of time possible or implement other affirmative measures to protect it to avoid an embarrassing and potentially costly data breach.

In addition to ISPs, operators of other electronic services, such as e-mail or interactive websites, may have data of investigative value to law enforcement. Such providers are typically referred to as "online service providers" or "OSPs." OSPs may have data sufficient to permit law enforcement to identify the user associated with a given communication (such as posting or downloading a video or sending

80 For example, a small business can purchase a static IP address from a provider so customers can always locate the company's site using the same World Wide Web uniform resource locator (URL).

81 *See* "wardriving" on http://en.wikipedia.org

an e-mail). So although the Congressional remit to this subcommittee (*supra*) uses arcane terms like "electronics communications service provider" and "remote computing service provider," this section of the report will use the more modern, Internet-era terms ISP and OSP.

ANALYSIS

The following three sections present the differing and at times inconsistent perspectives of the three major stakeholders in the data retention debate – law enforcement, Internet and online service providers, and consumer privacy advocates. These three sections were separately drafted by representatives of those stakeholder groups, and do not represent a consensus position of OSTWG.

LAW ENFORCEMENT PERSPECTIVE

Overall, industry is very supportive of law enforcement's efforts to investigate online crimes, especially crimes against children.[82] Two major difficulties, however, complicate industry's efforts to assist law enforcement. First, there exists no consensus as to what data should be retained, even across similar communication industries, and retention periods vary greatly.[83] If necessary data is no longer retained at the time law enforcement requests it, the investigation typically can go no further, regardless of how much a given ISP wants to help law enforcement. Second, although most ISPs are extremely responsive to law enforcement's requests, some ISPs lack the expertise or the resources necessary to fully assist law enforcement by providing timely, full responses to requests for information. In almost all cases, this inability to respond is not the result of an unwillingness to help law enforcement, but rather simply a lack of training or funding, especially for the smaller ISPs.

Data retention periods should be long enough to account for three significant complicating factors:

- First, child pornography collectors necessarily seek to avoid detection by law enforcement. Given the inherently secretive nature of the crime, there is often a gap in time between the commission of the offense and the discovery of the crime.
- Second, as online child exploitation investigations are sometimes international in scope, there is at times a lengthy delay before U.S. law enforcement obtains information about U.S. offenders from foreign law enforcement.[84] If the U.S. offenders' ISPs no longer retain the relevant data at the time U.S. law enforcement seeks it, those investigations dependent on Internet data will likely fail and offenders will escape liability for their crimes.[85]

82 The following discussion is conditioned by the fact that these are Internet-based crimes and crimes where relevant data is digital, as opposed to other investigations where Internet data is less central.

83 The absence of any consistent industry-wide practice to retain data for any uniform minimum duration creates uncertainty in the law enforcement community and frequently causes investigators to seek the issuance of lawful process compelling disclosure in hopes that some data may still be retained by any given provider. As discussed in the International Association of Chiefs of Police (IACP) resolution cited below, the creation of any uniform, industry-wide, minimum data retention duration practice would enable the law enforcement community to be more strategic in their requests, reserving inquiries primarily to those circumstances in which it is reasonable to believe that data would still be in existence at the time of the request.

84 Law enforcement recognizes that even if Congress were to mandate a retention period for IP address information, it would only apply to U.S.-based ISPs and OSPs.

85 As these investigations are often international in scope, it is appropriate to recognize that the European Union issued a data retention directive in 2006 generally requiring that EU member states ensure the retention of specified data for not less than six months or more than two years. See http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32006L0024:EN:HTML. It is also appropriate to recognize that some privacy advocates believe European privacy laws often better protect from disclosure to private parties the data subjected to this mandate than does U.S. law.

- Third, as online child exploitation investigations often involve an extremely large amount of data and government computer forensic resources are limited, when law enforcement seizes one offender's computer there often is a delay while that computer is examined for, among other things, leads about other offenders. Again, if those other offenders' ISPs no longer have relevant data at the time it is requested, those other offenders can go free. Particularly compelling are those investigations where law enforcement identifies a central source of child exploitation material working its way up the distribution chain from one known offender who received the material and who then re-distributed it.

The inability to identify those recipients due to the unavailability of critical provider data not only harms law enforcement's efforts, but also reinforces perceptions among child exploitation offenders of impunity and anonymity.

From a law enforcement perspective, the key challenge upon discovering an image of child pornography is determining who posted or transmitted the material. This requires linking together a string of data generated when a person goes online.

Because IP addresses are dynamically assigned (see above), it is critical to know the time zone in which the IP address of interest was located. For example, if at 3 PM a bomb threat is emailed to a school from a certain IP address in New York, and then an hour later the IP address gets dynamically reassigned to a customer in California, law enforcement could obtain inaccurate information if it queried the ISP and asked which customer had the IP address at 3 PM without specifying the time zone to which request referred, Eastern or Pacific. In the worst case, the answer would be incorrect and the police would pursue the wrong subscriber in search of their suspect.

The key to being able to link an illegal image to the person who sent or received it is the retention of the data at each stage of its transmission. First, the ISP used by the offender to access the Internet must retain the relevant data about the subscriber and the IP addresses he is assigned. Second, the OSP (such as Gmail or YouTube) that the offender used to post the video or send the e-mail must retain logs of the activity of IP addresses that have communicated with its services. If at any stage the necessary data is not retained, the investigation may come to an end and an offender could escape capture.

Therefore, in considering the creation of data retention rules, five basic issues must be addressed: (1) what data would need to be retained, (2) how long the data must be kept; (3) who would need to retain the data; (4) who would have access to the data retained, and under what conditions; and (5) what protections for consumers would be necessary.

1. What Data Would Need to Be Retained, and for How Long?

In order to complete their investigations, in general terms, law enforcement must be able to identify the subscriber or customer who was assigned a particular IP address by an ISP at a particular date, time, and time zone.

Moreover, law enforcement also must be able to identify an OSP's subscriber or customer. Like ISPs, OSPs should retain sufficient data to permit law enforcement to identify the user associated with a given communication (such as posting or downloading a file or sending an e-mail). The specific

categories of information that law enforcement may seek from OSPs parallel those sought from ISPs, but the investigative focus may be different. For example, a customer may provide inaccurate, or at least unverifiable, information when registering as a user of that OSP.[86] To provide a common example, an individual may use a false name when registering an email address with Gmail. Accordingly, the information likely to be of most investigative value includes information that the OSP user would not be able to falsify, such as records of session times and durations (i.e., when the user was logged on with that OSP) as well as IP address information.

Taken together, this data from ISPs and OSPs is referred to as "source data," that is, data that allows an investigator to trace back to the source of an electronic communication that constituted a crime on the Internet. It is this *combination* of information – both the IP address of the computer used to send the e-mail through a content or services provider and information about the ISP subscriber assigned the relevant IP address – that is critical to identifying a criminal on the Internet. If an online service provider, such as Gmail or Hotmail, does not retain connection or access data, an investigation will often be stymied at the very first step of the investigative process because law enforcement will not have enough information to take the next step of obtaining subscriber information through a subpoena to an ISP. Without the initial data point from the online service provider – often the first, crucial source of information relating to a crime – the trail of a criminal's activity on the Internet will turn cold and the investigation can end in failure.

A key variable in considering any data retention requirement is the length of time data would be retained. As noted above, current practices vary from company to company. Some retain it for less than 30 days, others for a period of months or years. Many crimes are not discovered until a significant period of time after they have been committed and, in some cases, the information critical to pursuing the case has been deleted by the time law enforcement authorities request it.[87]

2. Who Would Need to Retain the Data?

Any data retention requirement could cover three groups of companies, with slightly different requirements pertaining to each:

- First, ISPs providing Internet access to the public could be required to retain source data as described above. In fact, most ISPs already do retain source data for their own business purposes, but many do not do so consistently or for sufficiently long periods of time to be fully useful to law enforcement.
- Second, OSPs accessible by the public could be required to retain source data. Limited data retention requirements could be imposed only upon ISPs and OSPs that provide or offer a service to the general public for a commercial purpose, defined broadly. For example, it is a "commercial purpose" for a provider to offer the service free of charge to the user when the provider earns money from advertising, or when the provider obtains some other commercial benefit as a result of providing the service.
- Third, operators of "anonymous proxy" servers, whether commercial in nature or not, could be required to retain data concerning the communications they modify. Proxy servers are computers that receive, modify, and then retransmit Internet communications in a way that obscures the IP address used to originate the communication. That is, a proxy server assigns a user a different IP address than the one the ISP assigned to the user so that he could connect to the Internet in the first place. With that proxy IP address, the user can surf the Internet without anyone being able to trace his true identity. Those who operate proxy servers could be required to retain logs of the incoming IP addresses from their users (that is, the true IP address assigned by the ISP) and the outgoing IP addresses the proxy assigned (as well as the dates and times associated with their use) in order to permit effective investigations of offenders who use proxy servers to commit their online crimes.[88]

3. Who Would Have Access to Retained Data and Under What Conditions?

Without expressing an opinion on whether private litigants should have access to retained data, it is clear that law enforcement should have access to this data to investigate online crimes. With regard to government access to the data, it should be available on the same basis as other information on criminal suspects – that is, only through legal process such as a subpoena, search warrant, or court order.[89] This would provide an important protection for civil liberties both substantively and in terms of public perception. Furthermore, as with other legal process, a person served with process requesting retained data could be able to challenge that process in court. Such records are today covered by the Electronic Communications Privacy Act[90] (ECPA), which establishes a detailed set of rules for law enforcement access to these records.[91]

4. What Protections for Consumers Would Be Necessary?

Data retention is a controversial subject because of the perceived invasion of private information regarding individuals' Internet activity. As noted above, the requirement for legal process for access to that information protects Internet users, in large measure, from misuse by governmental authorities. However, an additional concern is the security of the retained data from misuse by third parties, either as a result of hacking or unintended disclosure. Possible solutions include: (1) the legislative creation of a federal privacy policy; (2) a prohibition on the commercial use of such data unless first rendered anonymous through an approved process; (3) a prohibition on the transfer or sale of such data; and (4) a requirement that providers have and publish a privacy policy, the violation of which would be a grounds for a breach of contract action or civil enforcement. Similarly, protection of data from hackers is also necessary. Again, various solutions are possible, including the legislative or regulatory creation of federal security standards, incentives or requirements for companies to develop security protections, or requirements that providers publish security policies, the violation of which would be a violation of their terms of service agreements.

5. Conclusions and Balancing Competing Concerns

Through the meeting of the OSTWG and otherwise, concerns have been raised by privacy advocates and members of industry about the need for mandatory data retention rules. While law enforcement respects the need for careful consideration of all issues prior to any legislation, law enforcement

86 Note that ISP users may also provide false names and stolen credit card information when applying for Internet service.

87 The United States Department of Justice has no official position on the issue of mandating data retention requirements. However, consistent with the October 2006 Resolution of the International Association of Chiefs of Police (IACP) which called upon all nations to enact uniform source and destination data retention requirements, the Federal Bureau of Investigation, has in the past publicly supported the retention by all public, commercial communications providers (i.e., Internet and telephony) of non-content information that would identify both the source and destination of communications for a uniform period of two years. See http://www.theiacp.org.

88 Of course, this could have the effect of driving some proxy server operators offshore, beyond the reach of U.S. law enforcemen

89 Among the exceptions to this rule are "exigent circumstances." Under 18 U.S.C. 2702(c)(4), a provider is permitted to disclose non-content records to the government "if the provider, in good faith, believes that an emergency involving danger of death or serious physical injury to any person requires disclosure without delay of information relating to the emergency." Under exigent circumstances, the provider gains information about an emergency, either from law enforcement, a customer, or in the routine operations of its business. The provider then has the authority to disclose the information to law enforcement to prevent harm to life and limb. This disclosure is optional, not mandatory, *i.e.*, the provider can disclose the user's information if it believes an emergency situation does exist, but it does not have to disclose.

90 18 U.S.C. §2510 *et seq.*

91 See 18 U.S.C. §§2702, 2703.

respectfully disagrees that a data retention law would inappropriately invade privacy or result in the harms that others have foreseen.

For example, some privacy advocates have asserted that the benefit of data retention to law enforcement would be short term, suggesting that criminals will move their data to foreign servers. Law enforcement disagrees that this is likely to occur. While some criminals are already utilizing foreign servers to avoid U.S. law enforcement access, they are unlikely to move out of the U.S. Thus, at a minimum, data retention requirements would help to identify those committing crimes inside the U.S. For example, when foreign law enforcement seizes a server to which U.S. offenders have uploaded child pornography images that they have made – as happens routinely today – American law enforcement officers will need data stored by American providers to be able to apprehend those criminals.

Privacy advocates have also raised a concern that if a newspaper were required to collect the IP address of a user who visits its web site, it would change users' online experience. This contention appears unfounded. Today, most websites routinely capture this sort of information for marketing and technical purposes. For example, according to the New York Times' privacy policy, their website collects "tracking information collected as you navigate through [their] sites" and requires users to supply their name and unique email address to get much of their content. *See* www.nytimes.com/ref/membercenter/help/privacysummary.html.

In addition, many advocates have pointed out the positive value of current data "preservation" laws that allow law enforcement to preserve data on a limited case-by-case basis (*see* 18 U.S.C. § 2703(f), as well as the preservation rules in the PROTECT Act). While these rules are undoubtedly helpful in many situations, they unfortunately do not adequately support the investigation of child exploitation and other crimes. As numerous law enforcement witnesses at the hearing described, this system completely fails in the many situations where a crime is not promptly reported, where evidence is obtained from foreign law enforcement, and where forensic delays prevent the tracing of the offender before the data has been deleted by the provider. For example, it is extremely common to seize a computer that shows that offenders have been making and distributing child pornography for an extended period, even years, but law enforcement can only act on the very recent offenses because providers have not retained data that would allow investigators to identify earlier offenders. In sum, while preservation of evidence on a per-case basis is undoubtedly helpful – its basic form has been the law for over 10 years – it is manifestly inadequate to meet this law enforcement need. There is therefore no reason to delay implementation of data retention rules on this basis.

Moreover, some have argued that data retention would create an extraordinarily costly burden for providers. While law enforcement agrees that cost issues need to be taken into account, the cost of storage of data has dropped exponentially. Accordingly, cost issues need not preclude a focused data retention requirement, as shown by the experience of mandatory data retention in Europe.

Some advocates also suggest that retained data would create a security risk and could be intentionally or unintentionally exposed. Law enforcement understands that many companies are already collecting many types of data at issue here and are already retaining it for marketing, billing, and other reasons (albeit for shorter periods of time than needed to facilitate online investigations). While companies would, of course, need to continue to take steps to secure retained data, such steps are not so different from the ones they already take, and law enforcement is not aware of significant problems that have occurred with this type of data to date.

Further, some privacy advocates have pointed out in their arguments against mandatory data retention that the Supreme Court has recognized that the First Amendment protects the right to speak anonymously. While this general principle may be true, the cases that they point to, such as *Talley v. California*, 362 U.S. 60 (1960) and *McIntyre v. Ohio Elections Commission*, 514 U.S. 334 (1995), state general principles and do not deal with a requirement that data be retained. Instead, in those cases, the Supreme Court examined situations where a law required the speaker to disclose *to the government* his or her identity. Those cases do not reach the issue of whether the government may investigate the authorship of speech. (Indeed, in *McIntyre* the Supreme Court noted that it was not, in fact, impossible for the government to track down the author of the speech to ensure compliance with other election laws at issue.) Moreover, it is important to understand that data retention would not automatically place any information into the hands of law enforcement officials. Of course, the First Amendment would continue to protect speakers by preventing any government action to obtain that data that did not comply with the Constitution.

Finally, some privacy advocates have suggested that if Congress were to enact even a limited data retention requirement, it would be virtually inevitable that data retention requirements would be expanded to more and more classes of information, including content. This claim is apparently based on the supposition that political and other pressures would follow "notorious unsolved crimes" that could have been solved if more data had been retained. First, it does not appear that any law enforcement group has suggested that ISPs be required to retain content. More importantly, this claim is contradicted by the current situation, in which much data is retained by providers but not universally or for long enough periods. No "enormous" pressure for data retention has occurred to cause the imposition of even limited data retention requirements, let alone some unlimited version predicted by these advocates.

In sum, while law enforcement understands the need to carefully consider all sides of this issue, and to give appropriate weight to the concerns expressed by our colleagues, law enforcement respectfully disagrees that data retention sufficient to facilitate the effective investigation of online crimes would be in any way unsound, illegal, or unworkable, and believes that better data retention will allow law enforcement to solve more crimes involving the sexual exploitation of children.

SERVICE PROVIDER PERSPECTIVE

The debate over mandatory data retention has been a persistent feature of the policy landscape for years. Internet access, online service providers, wireless carriers, telecommunications and cable companies, as well as privacy advocates, have expressed unified opposition to federal and state legislative proposals that would impose sweeping data retention requirements.

Service providers fully understand the importance of digital data in investigations of crimes against children, and (as implicitly acknowledged in the law enforcement perspective, *supra*) there is a long history of cooperation and engagement between industry and law enforcement to make available critical evidentiary data promptly and comprehensively in response to valid legal process.

While opposing data retention mandates, service providers have consistently supported data preservation as a more efficient, reliable, and sensible method for making Internet and other digital records available for use in criminal investigations.

Representatives of service providers participating in the OSTWG Subcommittee on Data Retention

continue to oppose mandatory data retention requirements as overbroad, unnecessary, ineffective, and premature – particularly at this point in time (as explained below).

1. Congress should assess the effectiveness of the new data preservation requirements of the PROTECT Our Children Act before considering mandatory data retention.

In the Child Pornography Reporting section of this report, that subcommittee has summarized the data preservation requirements enacted recently by Congress in the PROTECT Our Children Act.[92] The new reporting and data preservation provisions, codified in 18 U.S.C. § 2258A, detail the information that service providers now include in their required reports of apparent child pornography crimes to NCMEC's CyberTipline – including the types of digital records that law enforcement considers critical to identifying the perpetrators of crimes against children.

This data includes identifying information concerning the individual who appears to have committed the crime (such as email address, Internet Protocol address, and any self-reported identifying information); information as to when and how a subscriber uploaded, transmitted, or received apparent child pornography, or when and how it was reported to or discovered by the provider; geographic location information, such as a billing address, zip code, or Internet Protocol address; the image of apparent child pornography; and the complete communication containing the image, including data relating to its transmission and other data or files contained in or attached to the communication.

Mandatory data retention is therefore a non-issue with respect to the data accompanying CyberTipline reports, since key information is delivered directly to NCMEC and forwarded to law enforcement even before a criminal investigation has begun.

The PROTECT Our Children Act goes a step further, however, requiring service providers to preserve for 90 days not just the CyberTipline report but also additional data that Congress determined to be important for investigating crimes against children. Subsection (h) of 18 U.S.C. § 2258A requires service providers to treat NCMEC's notification of receipt of a CyberTipline report as a request to preserve subscriber information under 18 U.S.C. § 2703(f), a well-established procedure (discussed below) that law enforcement routinely employs to prevent the deletion or overwriting of data in a subscriber's account pending issuance of legal process. The new provision requires service providers to preserve any images or files commingled or interspersed among the images of apparent child pornography within a particular electronic communication or user-created folder or directory.

The data preservation provisions of the PROTECT Our Children Act are focused and well thought-out. Congress should give this approach a chance to work, and should carefully assess its effectiveness after law enforcement has had a reasonable period of first-hand experience using the accumulated data in the investigation and prosecution of crimes against children. Only if data preservation has been shown to be ineffective should Congress consider weighing the benefits and drawbacks of the much broader and less focused scheme of mandatory data retention under discussion by this subcommittee.

2. Service providers encourage law enforcement to take advantage of the powerful tool available under ECPA.

As noted above, 18 U.S.C. § 2703(f), referenced in the PROTECT Our Children Act, already establishes a mandatory data preservation process that law enforcement has used in a wide range of digital crime investigations (not limited to crimes against children) since its enactment in 1996.

92 P.L. 110-401, Title V ("Securing Adolescents from Online Exploitation"), § 501(a), 122 Stat. 4229 (October 13, 2008). The alternative short title of P.L. 110-401 is the Providing Resources, Officers, and Technology To Eradicate Cyber Threats to Our Children Act of 2008.

The provisions of § 2703(f) are concise: upon the request of law enforcement, a service provider "shall take all necessary steps to preserve records and other evidence in its possession pending the issuance of a court order or other process," and shall retain such records for a period of 90 days, which shall be extended for another 90 days upon a renewed request by law enforcement.

Data preservation under this statutory procedure is mandatory and straightforward. Any governmental department or agency, local, state, or federal, may issue a preservation request to a service provider. No judicial action or court order is required, there is no factual showing of relevance or materiality, and no other evidentiary standard must be met.

The subcommittee heard conflicting views from law enforcement about the utility of existing data preservation authority. From the service providers' perspective the data preservation approach strikes the right balance by permitting providers to determine the optimal duration of data retention based on their business needs, while requiring them to preserve data upon request under § 2703(f).

3. Mandatory data retention will encompass vast swaths of customer data that will rarely be sought by law enforcement and prove useful in very few criminal cases, while presenting unacceptable risks to privacy and security.

Although policy discussions of data retention always generate controversy, all participants can agree on certain facts. There is no question that the vast majority of Internet users will never commit crimes, and for those who do, Internet data is likely to be irrelevant to most of those crimes. Therefore, it is indisputable that, if data retention is required by law, most of the huge mass of data collected and stored by every provider, closely tracking their customers' Internet identities, relationships, and activities, will never be useful in a criminal investigation and will never be sought by law enforcement.

Because providers would bear the costs of collecting, storing, and retrieving data for up to an estimated 230 million Internet users in the United States alone,[93] the usefulness of the infinitesimally small proportion of data that might someday be sought for a specific criminal investigation has to be weighed against the inefficiency and risks of wholesale data retention.

Internet data retention is a model that would not make sense in any other context. It is unimaginable that laws would ever require private persons to "retain" physical information such as fingerprints, left anywhere by anyone, on the chance that someday they would prove relevant to a criminal investigation. Any such law would rightly be seen as grossly out of proportion, in disadvantages and costs, to its possible value in solving crimes. When its real-world implications are examined, the value of Internet data retention envisioned by its proponents is similarly out of proportion to its disadvantages and costs.

A threshold problem in enacting mandatory data retention is how to identify, by statute, the range and type of data that providers are required to collect, store and maintain. Law enforcement in its discussion, *supra*, identifies some of the data that is currently used in criminal investigations, but Internet technology evolves rapidly and the data that is relevant today may become obsolete and irrelevant tomorrow. Legislating retention of a static set of mandatory data might limit providers' capacity to retain data generated by new products and services that might prove helpful to future investigations. Sophisticated criminals would thus have incentives to move their Internet activities to newer services that may not be encompassed in existing legislative mandates.

93 Estimate of the International Telecommunications Union for 2008, available at http://www.itu.int/ITU-D/ict/statistics/

Even assuming it could be identified in statutory language that is fortified against obsolescence by technology and evasion by criminals, the data collected by every provider must be searchable by practical means. Moreover, the results of every search must be accurate. Neither of these requirements is addressed in any rigorous way by proponents of data retention. The processing power necessary to search through exabytes of data[94] will be enormous and unprecedented, and it is not clear that every organization offering Internet access or online content in the United States will have the resources to build systems capable of undertaking such searches. Nor is it clear that accuracy can reasonably be assured when operating on databases of this expected magnitude, particularly when each provider will employ different storage and retrieval systems of varying capabilities. When human error is also factored in, mistakes may occur resulting in wrongful searches and seizures and creating potential civil liability for both providers and law enforcement officials.

Law enforcement's discussion of proxy servers *supra* is illustrative because it magnifies both of the foregoing problems inherent in wholesale data retention. Proxy servers are not offered solely to provide anonymous web surfing but are used to bring other innovative services to customers, including caching and content filtering, particularly to those millions of users who use dial-up services. Providers employing proxy servers, however, would be placed at a serious disadvantage by mandatory data retention simply because the data volumes generated by sharing IP addresses (for example) is orders of magnitude greater than assigning single, Internet-accessible IP addresses to each user. Organizations that employ proxy servers or other protocols such as network address translation – including wireless communications providers, government agencies, employers, schools, universities, libraries, hotels, airports, coffee houses, and municipalities offering public Wi-Fi hotspots – would therefore be weighed down by even greater resource demands than other providers.

Apart from its lack of practicality or usefulness in most criminal cases, amassing huge databases of personal information about nearly every American using the Internet would present new and unparalleled risks to privacy and security. The existence of disparate and widely dispersed databases encompassing our Internet identities, contacts, relationships, and communications, some of which inevitably will be poorly secured, could be fairly characterized as an "attractive nuisance" in proportion to their increasing scale and depth. The potential harm posed by unauthorized access to these troves of data is limited only by the imaginations of hackers, cybercriminals, foreign agents, and other malefactors.

Therefore, according to the law enforcement perspective, service providers would have to be subjected to a new and unprecedented regulatory regime to ensure that neither the providers themselves, nor the increasingly smarter cybercriminals, gain access to or use this voluminous data for unsanctioned purposes. Law enforcement suggests that Congress should be called upon to create overarching federal privacy policies with new prohibitions on commercial use, transfer or sale of the data, enforced against providers by breach of contract or other civil actions carrying the threat of liability for fines and damages. Similarly, law enforcement recommends congressional action to impose upon providers federal cybersecurity requirements made necessary by mandatory data retention, to be enforced in the event of violations by breach of contract or civil enforcement actions against those providers.

94 Each exabyte equals one million trillion bytes. One expert estimates that, as of March 2010, the global flow of information over wired and wireless networks totals 21 exabytes per month. Padmasree Warrior, Chief Technology Officer of Cisco Systems, speaking at the International CTIA Wireless show on March 24, 2010, quoted in Michael Miller, PC Magazine, http://www.pcmag.com/article2/0,2817,2361820,00.asp (visited May 2, 2010).

In light of its limited usefulness for criminal investigations, there is no way to justify either the risks posed by the massive accumulation of sensitive personal data, or the far-reaching extension of government regulatory power over the Internet that mandatory data retention would necessitate.

4. Summary of Service Provider Perspective

Congress should first assess the impact of the more focused and efficient data preservation procedures enacted in the PROTECT Our Children Act before considering mandatory data retention. Absent compelling reasons justifying the indiscriminate collection of data that is inherent in any broad-based data retention scheme, its drawbacks and risks far outweigh any perceived utility. Requiring service providers to retain trillions of digital records over a period of years, when none but a tiny fraction of those records will ever be relevant to any criminal investigation, will not significantly contribute to the prevention, detection, or prosecution of crimes against children. It will almost certainly create substantial risks to personal privacy and security, and give rise to regulatory and liability schemes that will weigh heavily on service providers in an already challenging economic environment, without providing tangible benefits to law enforcement in most cases.

PRIVACY PERSPECTIVE

A broad, pervasive scheme of mandated data retention by all entities in the United States that provide Internet access or that offer goods or services on the Internet would damage privacy interests and free speech on the Internet.[95] While it could benefit law enforcement in the short term, child pornographers – both distributors and users – would adjust their conduct to evade or minimize the impact of such a mandate. For example, a broad mandate could drive to offshore servers the same troublesome content now hosted in the United States; it would be accessed through offshore anonymizers not subject to the data retention requirements imposed in the U.S. A data retention mandate would also do little, ultimately, to stop the worst of the worst, and it would fundamentally change the Internet experience for people in the United States engaging in entirely lawful activity by burdening the curious and quieting the controversial. Once users understand that their Internet usage is tracked and retained, they will be less free in exploring alternative ideas available online. It would also increase the privacy impact of the inadequacies in current law which unnecessarily put privacy at risk by making more data accessible to law enforcement under low standards and inadequate process. For these reasons, the privacy community opposes mandatory data retention.

Beyond privacy and free speech concerns raised by the retention itself, data retention mandates raise serious questions about whether such retention is technically feasible and who would bear the costs of such retention. A mandate that ISPs retain IP address allocations would impose significant costs on those providers. A mandate that the other end of Internet communications – the web-based and other servers and services that citizens visit and use (provided by on-line service providers or OSPs) – retain IP addresses and other information would be an overwhelming and extraordinarily costly burden – and would certainly lead to the reduction in content and services available on the Internet. This would in turn raise serious constitutional concerns.

95 Although the Law Enforcement Perspective above disclaims intent to force all online sites to retain information, law enforcement makes clear that they want to track and monitor any website that allows users to communicate with other users. In the modern Web 2.0 world, however, that encompasses the vast majority of new and popular websites. Most new sites that offer goods and services allow users to post feedback or otherwise exchange information, and this will only increase as more sites are integrated with social networking services. Most modern sites, large and small, commercial and non-commercial, would ultimately be covered by law enforcement's proposed data retention mandates.

1. The First Principle of Data Privacy

Data retention mandates run headlong into the first principle of privacy: if the data isn't there, its privacy cannot be compromised. Currently, businesses save the data that is useful for the operation of their business, and they dispose of data that is not useful. In the case of IP address allocations, some ISPs find a longer period of retention necessary than do others. Some hold payroll data longer than do others. Some hold employee personnel records longer than do others. All of this data, and more, would be useful to law enforcement investigating some types of crime. The longer any of this data is maintained, the more at risk it is to compromise by the nefarious, or to inadvertent disclosure by the careless.

2. Preference for Targeted Data Preservation Requests

Data retention mandates would affect all users, not just the bad actors. That means that the vast majority of people whose privacy would be put at risk are innocent citizens. A far better approach – targeting the data of suspects – can be found in current law.[96] It permits law enforcement and any other governmental entity, without any judicial permission or notice at all, to require an ISP to retain data – including IP address and customer identifying information – for 90 days. The law requires no supervisory approval and no finding even within the requesting agency of specific facts that the records to be preserved are relevant to an investigation. Another 90-day period is available upon request of law enforcement. Law enforcement typically uses this power when it has identified an investigative target. In the child pornography context, current law requires that service providers *automatically* retain information whenever they make a report of possible child pornography to the National Center for Missing and Exploited Children (NCMEC).[97]

The privacy and civil liberties benefit of this approach are enormous: data about only the tiny fraction of individuals who have fallen under criminal suspicion is subject to a data preservation requirement. Everyone else would continue to enjoy the same level of privacy he or she would otherwise enjoy regardless of the law enforcement investigation. Instead of requiring ISPs and others to retain data primarily about people under no suspicion, law enforcement should focus on ways to ensure preservation of data about people who are under suspicion. For example, law enforcement should have additional resources – particularly in the computer forensics area – so that when a computer of a child pornography suspect is seized, it can more quickly be analyzed for leads on other offenders. This would help law enforcement quickly identify the data it needs and the entity holding the data so that a preservation order can promptly be issued. The solution to inadequate computer forensic resources should be to increase those resources, rather than to subject more data of innocent users to risk.

3. Inadequate Standards for Law Enforcement Access

Proposals to mandate data retention cannot be viewed in a legal vacuum. The privacy impact of data retention proposals must be assessed in light of the very limited privacy protections that are currently afforded to the data that would be retained. For this reason, reliance on the existing requirements

96 18 U.S.C. 2703(f), Requirement to preserve evidence, provides:

1. **In general.** – A provider of wire or electronic communication services or a remote computing service, upon request of a government entity, shall take all necessary steps to preserve records an other evidence in its possession pending the issuance of a court order o other process.
2. **Period of retention.** – Records referred to in paragraph (1) shall be retained for a period of 90 days, which shall be extended for an additional 90-day periods upon a renewed request by the governmental entity.

97 Of course, as described above in the law enforcement perspective section, the authority to preserve data does not help in cases where the crime is not immediately reported or where law enforcement uncovers data of earlier crimes.

of legal process to protect the privacy of data that would be subject to the retention mandate is misplaced.

Data retention mandates may be imposed on IP addresses and corresponding user identifying information (name, address, credit card and bank account number); this data is available with a subpoena and no notice need be made to the record subject.[98] For example, transactional data about everyone who viewed a particular web page is available with only a subpoena and without judicial oversight, even though such information (except child pornography) can be particularly sensitive. The legal process in this instance involves no proof of specific facts, no judge, and no opportunity for the record subject to object for any reason – yet reveals what content people have viewed even though they may not be targets of an investigation.

As a result, law enforcement requests for such inadequately protected data can target people who are likely entirely innocent. Were websites and other OSPs required to retain data on visitors, such information would be subject to a mere subpoena, which could, for example, be issued to require a covered provider supply identifying information about every person viewing a particular Web site. Although one could argue that this would be acceptable if the web site contained child pornography, the problem is that any data retention mandate would apply to *all* OSPs, including sites that provide sensitive, controversial, or unpopular but nevertheless lawful and constitutionally-protected content.

Take for example the person who views "jihadi websites" that glorify terrorism. Such person might be a terrorist, an opponent of terrorism, a student doing a research paper, or a person who is curious. A subpoena seeking user identifying information for every person who viewed that website – which could be followed by knock on the door or other investigative activity focused those who viewed the content – would have an obvious negative impact on free inquiry, and on free speech.

4. Extending Data Retention Mandates To On-Line Service Providers

Law enforcement has made it clear that it wants data retention mandates to reach beyond ISP access providers (which are the only entities that supply dynamic or static IP addresses) to *also* apply to OSPs. For example, YouTube is an OSP – its advertising-based sales model permits users to freely upload and view videos. Barnes and Noble is an OSP, offering for sale books and other written materials both on-line and in its brick-and-mortar stores, and invites readers to communicate with each other about the books it makes available.

Law enforcement has argued that, to be effective, a data retention mandate must apply both to ISPs and to OSPs. Otherwise, it is argued, the identifying data from the ISP cannot be linked to "crime scene" data obtained by the OSP. But a data retention mandate on an OSP news outlet like the New York Times or a video sharing service like YouTube has an enormous societal cost that must be considered. Of course, a person can post a comment on the New York Times website that consists of child pornography. But requiring the New York Times to maintain records of whenever *any* user was signed on and of the IP address used changes the on-line experience. When such a practice is disclosed to the user – as it must be – it tells the user that what he or she says is being watched and possibly saved, in a way that can be traced back by the user for later retrieval by law enforcement, all without judicial authorization and without so much as notice to the user. This would chill public discourse and encourage self-censorship at the expense of robust public debate.

98 18 U.S.C. 2703(c)(2) and 18 U.S.C. 2703(c)(3).

5. Data Retention and Anonymity

Anonymity fosters public discourse and political debate. The Federalist Papers – documents key to the founding of the United States – were published anonymously under the pseudonym "Publius," including papers authored by James Madison, John Jay and Alexander Hamilton. The James Madisons of today are no more likely to deal in child pornography than the James Madison who became President. Yet, a data retention mandate would be by definition indiscriminate and over-inclusive: it would apply to the criminal and the victim, to the politician and the dissident. Law enforcement officials use IP address and date/time stamps to associate communications with particular ISP subscribers. Because it is impossible to discern in advance the IP addresses and date/time stamps that will pertain to criminal – as opposed to lawful – conduct, a data retention mandate must cover all data.

The Supreme Court has repeatedly recognized that the First Amendment protects the right to speak anonymously. In *Talley v. California*, 362 U.S. 60 (1960), the Court said, "Anonymous pamphlets, leaflets, brochures and even books have played an important role in the progress of mankind." In *McIntyre v. Ohio Elections Commission*, 514 U.S. 334 (1995), the Supreme Court said, "Protections for anonymous speech are vital to democratic discourse. Allowing dissenters to shield their identities frees them to express critical, minority views...." Data retention mandates would diminish the possibility of engaging in anonymous speech. The very purpose of requiring ISPs and OSPs to retain IP address and date/time stamp information is to eliminate the possibility of anonymous speech, by ensuring that speech can be traced back to the person who uttered it.

6. The Steep Cliff

While some law enforcement officials have called only for mandatory retention of IP address, date/time stamps, and subscriber identifying information by ISPs to allow law enforcement to link a communication to a real person, others have made broader demands. Some seek to impose data retention requirements not only on ISPs, but on OSPs as well. Others would extend data retention mandates to more classes of data, and include even content, and have it retained for a much longer time.

It seems inevitable that once a line is crossed to mandate data retention for a limited class of data (e.g., IP address, date/time stamp, and subscriber identifying information) and a limited class of holders of that data (e.g., ISPs only), it is virtually inevitable that the data retention mandate would expand because of pressure that follows notorious unsolved crimes. If, for example, an OSP deleted records of session times, session duration, and IP address that would have identified a notorious criminal who used the OSP service for a particularly terrible crime, the pressure to require retention of such data would be enormous.

This is not just a "slippery slope" problem; it is a steep cliff problem. Once the boulder begins to fall from the top of that cliff, virtually nothing can stop it from reaching its logical resting place. In this case, the logical resting place for data retention mandates is a requirement to save content that extends not only to ISPs, but to all entities that provide services on line. In *reductio ad absurdum*, ISPs and OSPs would retain everything emanating from an end-user's computer for all time – clearly an untenable solution and lacking the requisite balance between law enforcement's legitimate needs and users' privacy rights.

7. Privacy Summary

It is clear from the discussion above that there is no current consensus on whether or how there should be mandated data retention. But there are a number of areas in which progress can be made to help law enforcement fight online crime without requiring onerous and burdensome data retention.

CONCLUSION

In the end, data retention is about striking a balance between (1) law enforcement's legitimate need to investigate and prosecute crimes against children carried out or facilitated by the Internet; (2) end-users' legitimate privacy expectations and the democratic ideals of anonymous and free speech; and (3) ISP/OSP costs of retention, costs that ultimately get passed onto consumers and, if these costs were to become onerous, could have the effect of stifling innovation and creativity on the Internet. Today, there is no clear consensus, as the foregoing sections have demonstrated, on how best to improve that balance. Here are some steps that could be considered:

- The ICAC task forces (there are 61 spread across the U.S.) hold regular meetings. ISPs and OSPs should have similar meetings, and joint meetings between the two groups, as well as federal law enforcement agencies, could take place quarterly or semi-annually. These meetings would be a means for industry and law enforcement to share information about emerging threats, resolve operational glitches, and develop new practices and procedures, if necessary.
- Consumers have their privacy expectations, and vast amounts of stored data raise significant privacy concerns.
- The data retention debate, if there is to be one, should take place at the federal level. As the foregoing perspective sections indicate, there is no consensus among the three major stakeholders on what data retention rules should be. If states are allowed to set their own data retention standards, this would burden the ISPs/OSPs with as many as 54 different sets of requirements, creating even more uncertainty for law enforcement.
- Congress should first assess the impact of the more focused and efficient data preservation procedures enacted in the PROTECT Our Children Act before considering mandatory data retention.

In summary, assessing the necessary balance between the retention needs of law enforcement, the requirements of ISPs/OSPs, and the privacy interests of consumers is a complex area. The subcommittee recommends that Congress carefully consider these often competing concerns before considering data retention rules.

APPENDIX A

The Online Safety and Technology Working Group wishes to thank the following people for generously giving of their time to assist us in our work:

Ellen Agress
Joe Alhadeff
Nathan Andersen
Carolyn Atwell-Davis
Traci Beagley
Jacqueline Beauchere
Cliff Boro
Bonnie Bracey
David Burt
Karen Cator
Ann Cavoukian
Michelle Collins
Chad Coons, Jr.
Chuck Cosson
Kate Dean
Norris Dickard
Leslie Dunlap
Kelli Emerick
Don Eyer
David Finnegan
Jorge Flores
Dona Fraser
Jill Geigle
Matt Gerst
Emily Hancock
Pamela Jones Harbour
Mary Heston
Julie Inman-Grant
Jasmine Johnson
Rick Lane
Jennifer Leach
Sally Linford
Emma Llanso
John Logalbo
Cynthia Logan
Roarke Lynch
Edwinna Lyuck
Carol Magid
Phyllis Marcus
Allan McCullough
Tim McShane
Eliot Mizrachi
Greg Nojeim
Lindsey Olson
Julia Plonowski
Cheryl Preston
Jason Rzepka
Kim Scanlan
Kim Scardino
Kristen Schoenenberger
Jamie Marie Schumacher
Stephen Sharon
Allan Smart
Rick Smith
Chris Stetkiewicz
Margaret Sullivan
Catherine Davis Teitelbaum
Frank Torres
Chris White
Art Wolinsky
Lori Wood

APPENDIX B

AGENDAS OF OSTWG MEETINGS

JUNE 4, 2009

Introductory Meeting

Location: Federal Communications Commission Meeting Room
445 12th St. SW, Washington, DC 20554

Time: 10 am to 2 pm

AGENDA

10:00-10:10 Call to Order and Welcoming Remarks by OSTWG Co-Chairs Anne Collier and Hemanshu Nigam

10:10-10:20 Opening Remarks by Anna M. Gomez, Acting Assistant Secretary of Commerce for Communications and Information

10:20-10:35 Remarks by Susan Crawford, Special Assistant to the President on Science Technology & Innovation

10:35-11:00 Video Presentation of Recorded Talk by KSU Professor Michael Wesch, given at the Library of Congress

11:00-11:30 Introductions by Working Group Members (going "around the table")

11:30 to 11:45 Break

11:45-12:30 Remarks by Federal Government representatives (FCC, FTC, DOJ, and Education) on government role and online safety work to date

12:30-1:30 Remarks by Subcommittee Chairs
a) Education Subcommittee (Larry Magid)
b) Data Retention Subcommittee (Michael McKeehan)
c) Child Pornography Reporting Subcommittee (Chris Bubb)
d) Protection Technology Subcommittee (Adam Thierer)

1:30-2:00 Closing Discussion

2:00 Adjournment

SEPTEMBER 24, 2009

Meeting on Internet Safety Education

Location: U.S. Department of Commerce Room 4830
1401 Constitution Ave. NW, Washington, DC

Time: 9 am to 4:30 pm

AGENDA

9:00-9:30 Welcome and Opening Remarks by OSTWG Co-Chairs Anne Collier and Hemu Nigam and Assistant Secretary of Commerce Larry E. Strickling

9:30-9:35 Introduction by Subcommittee Chair Larry Magid

9:35-10:20 Student Panel – D.C. public school students

10:20-10:30 Break

10:30-11:00 How Industry Educates, Stephen Balkam, Family Online Safety Institute

11:00-11:30 How Schools Educate, Nancy Willard, Center for Safe and Responsible Internet Use

11:30-12:00 Cyberbullying – local case study, Mike Donlin, Seattle Public Schools

12:00 Lunch Break

12:30-12:35 Welcome and Introductions, Danny Weitzner, Associate Administrator, NTIA Office of Policy Analysis and Development

12:35-1:05 Jessica Gonzalez, consultant to National Hispanic Media Coalition, on Hate Crime

1:05-2:00 How NGOs Educate (OSTWG members plus special NGO guests)

2:00-2:30 Risk Prevention Education in the Online Environment – Patti Agatston, PhD, Cobb County (GA) Schools

2:30-3:00 Digital Citizenship & Media Literacy Education, Alan Simpson, Common Sense Media

3:00-3:45 How Youth are Using Social Media, Prof. Henry Jenkins, Ph.D., University of Southern California

3:45-4:30 General Discussion

4:30 Adjournment

NOVEMBER 3, 2009

Meeting on Parental Controls, Child Protection Technologies, and Content Rating Methods

Location: U.S. Department of Commerce Room 4830
1401 Constitution Ave. NW, Washington, DC

Time: 8:30 am to 5 pm

AGENDA

8:30-8:45 Welcoming Remarks, Lawrence E. Strickling, Assistant Secretary of Commerce for Communications and Information

8:45-9:00 Opening remarks from Rep. Debbie Wasserman Schultz

9:00-11:15 Panel 1: Network-based & Independent-Provided Online Safety Tools

Moderator: Adam Thierer
Discussants: Karen Hullenbaugh, Director of Safety Products, AOL; Dane Snowden, Vice President, External and State Affairs, CTIA–The Wireless Association; Forrest Collier, Chairman & CEO InternetSafety.com/Safe Eyes; Rob Stoddard, Senior VP, Communications & Public Affairs, National Cable & Telecommunications Association; James Dirksen, Managing Director, RuleSpace; Marian Merritt, Internet Safety Advocate, Symantec; Cheryl Preston, Brigham Young University Law School and Think Atomic; Kevin Rupy, Director of Policy Development, USTelecom

11:15-11:30 Break

11:30-12:00 Panel 2: OS-level, Browser-based & Search-Oriented Tools & Methods

Moderator: Adam Thierer
Discussants: Frank Torres, Director of Consumer Affairs, Microsoft; Scott Rubin, Global Communications & Public Affairs, Google; Emily Hancock, Senior Legal Director, Yahoo!

12:00-12:30 Lunch Break

12:30-1:00 Luncheon Remarks from Will Gardner, CEO, Childnet International in London and Dr. Hoda Baraka, First Deputy, Egyptian Minister of Communications and Information Technology

1:00-2:30 Panel 3: Social Networking and Web 2.0 Approaches to Online Safety

Moderator: Tim Lordan
Discussants: Phyllis Marcus, Senior Staff Attorney, Federal Trade Commission; Jill Nissen, Vice President, Chief Policy Officer, Ning; Susan Fox, VP, Government Relations, Walt Disney Company/Club Penguin; Reggie Davis, General Counsel, Zynga

2:30-2:45 Break

2:45-4:00 Panel 4: Other Perspectives on Tools, Ratings & Online Child Protection

Moderator: Tim Lordan
Discussants: Todd Haiken, Senior Manager of Policy, Common Sense Media; Pat Vance, President, Entertainment Software Rating Board; Kim Mathews, Attorney Advisor, Media Bureau, Policy Division, Federal Communications Commission; Orit Michiel, Vice President and Domestic Counsel, Motion Picture Association of America; Stuart Rosove, Vice President for Media & Entertainment, Digimarc

4:00-4:30 "Digital Ethics Among Digital Youth," a talk by Carrie James, PhD, of the Harvard School of Education's GoodPlay Project

4:30-5:00 General Discussion

5:00 Adjournment

FEBRUARY 4, 2009

Meeting of the Child Pornography Reporting and Data Retention Subcommittees

Location: U.S. Department of Commerce Room 4830
1401 Constitution Ave. NW, Washington, DC

Time: 8:40 am to 5 pm

AGENDA

8:40-9:00 Opening remarks from Co-Chairs Anne Collier, Hemanshu Nigam, and Deputy Assistant Secretary of Commerce Anna Gomez

9:00-9:05 Opening remarks from Subcommittee Chair Chris Bubb

9:05-9:30 "Social Media Trends," Amanda Lenhart, Pew Internet and American Life Center

9:30-10:00 "CP Reporting 101," John Shehan, NCMEC

10:00-11:10 Law Enforcement Panel and Discussion

Bob O'Leary (Moderator); Drew Oosterbaan, Chief, CEOS, Department of Justice; Nicholas Savage, FBI SSA; Gerard F. Meyers, SAIC Iowa Internet Crimes Against Children Taskforce

11:10-11:20 Break

11:20-12:30 Industry Panel and Discussion

Kate Dean, USISPA (moderator); Chris Bubb, AO; Elizabeth Banker, Yahoo!; Frank Torres, Microsoft; Jill Nissen, Ning; Brooke Batton, United Online; Michael Sussman, Perkins Coie

12:30-1:15 Lunch Break

1:15-1:20 Opening Remarks from Data Retention Subcommittee Chair Mike McKeehan

1:20-1:45 "What, Exactly, Do we Mean by Data Retention?" Drew Arena, Verizon

1:45-3:05 Law Enforcement Panel And Discussion

Paul Almanza, Department of Justice (Moderator); Matt Dunn, Department of Homeland Security/ICE; Dr. Frank Kardasz, AZ ICAC; Gerard Meyers, Iowa ICAC; Gregg Motta, FBI

3:05-3:15 Break

3:15-4:25 Panel and Discussion: "Data Retention in Practice: Industry and Privacy/Civil Liberties Perspective"

Declan McCullagh, CNET (Moderator); Kate Dean, USISPA; John Morris, Center for Democracy & Technology; Chris Calabrese, ACLU; Dave McClure, USIIA; John Sevier, Davis Wright Tremaine

4:25-5:00 General Discussion

5:00 Adjournment

MAY 19, 2009

Final OSTWG Meeting

Location: U.S. Department of Commerce Room 4830
1401 Constitution Ave. NW, Washington, DC

Time: 1:30 pm to 5 pm

AGENDA

1:30-4:00 Opening Remarks from Hemanshu Nigam and Anne Collier, OSTWG Co-Chairs, and Lawrence E. Strickling, Assistant Secretary of Commerce for Communications and Information

1:40-3:00 Review and Refine Subcommittee Recommendations and Report Language

3:00-3:10 Opportunity for Public Comment

3:10-3:25 Break

3:25-4:45 Continuation of Report Review

4:45-5:00 Opportunity for Public Comment

5:00 Adjournment

APPENDIX C

STATEMENTS OF OSTWG MEMBERS

Parry Aftab (WiredSafety) Statement - OSTWG Report (full version – aftab.com/ostwg)

It has been an honor to serve on the OSTWG, a varied and stellar group. Each brings something special to the table. Because WiredSafety and my experience, especially our work with victims, parents and young people, differs from that of many working group members[1], while we concur with most of the conclusions reached in the Report, we differ on several others.

The most significant differences relate to the importance of law enforcement and the scope and prevalence of cyberbullying (where one minor uses digital technologies as a weapon to hurt another minor), "sexting" (taking, sending or possessing nude or sexual images of minors by minors, including of themselves) and sexual exploitation of minors by adults that is facilitated by digital technology. Based upon our 15 years in the field, we believe that more minors are victimized, victimizing each other and putting themselves at risk than the Report reflects. Things that are obvious face-to-face are less obvious online. While we agree that the education of young people about safe and responsible digital technology use is critical, under the right set of circumstances even a well-educated child could become an unwitting victim. It is the role of our police to keep this from happening. That is why we shouldn't lose track of the importance of well-trained and equipped law enforcement agencies and their role in our children's safety online and off.

At the same time, we recognize that the public (and parents, in particular) often over-estimate the risks children face online, especially when sexual predators are involved. (We fear what we don't understand, which is why parental education is so important.) While we have to correct their misconceptions, under-estimating the risks is not the answer. In our opinion, the Report leaves the impression that our young people are less at risk than our experience leads us to believe. How serious are the risks? Sadly, we can only guess. When it comes to cyberbullying, sexting and sexual exploitation of minors facilitated by digital technologies, we don't really understand the facts. We don't know how often they occur, to whom they occur and the seriousness of the victimization/harm. Why? Because our children often don't understand that they have been victimized, intentionally hide the victimization from us or don't share the truth when asked by researchers conducting academic surveys. (Only 5% of students polled told us that they would tell their parents if cyberbullied.) While under-reporting is an offline reality, it is worse when young people feel they have been complicit in some part of the digital abuse.

We are among the experts who believe that cyberbullying is at "epidemic levels" especially in middle school, and that more minors and at increasingly younger ages are engaged in taking, sending or receiving nude or sexual images. (Our survey of children 10 -12 disclosed that 5% had sent a sexually provocative, nude or sexual image and 6% had received one. Teenangels.org/sexting.) The MTV/AP survey conducted for the digital abuse prevention campaign, athinline.org (for which one of my Teenangels and I are advisory board members), shows a higher incidence of sexting than reflected in the Report, as well. This is particularly concerning, as those admitting to sending a "sext" also admitted to being more than 3 times more likely to consider suicide. The more we know, the better job we will be able to do. For that we have to engage young people, ask the right questions and demand better answers.

[1] WiredSafety served on the Harvard Berkman Center's ISTTF. It and I bring knowledge of cybercrime, law, privacy, best practices, victim-assistance, youth leadership and peer-education, parent education, mommy blogging and issues involving cyberbullying and the digital technology social and sexual conduct of minors. (To learn more visit WiredSafety.org.)

U.S. Department of Justice Addendum to the OSTWG Report

The U.S. Department of Justice ("Department") was pleased to contribute to the OSWTG process. This Addendum, concerning one issue, should not be interpreted to mean that the Department necessarily endorses the remainder of the OSTWG Report.

By stating that "several studies, including some funded by the U.S. Department of Justice, have shown that the statistical probability of a young person being physically harmed by an adult who they first met online is extremely low," the Report's Education Section could be read to indicate that the risk that online sexual predators pose to children is very small.[1] The research by the Crimes against Children Research Center ("CCRC") of the University of New Hampshire discussed in this portion of the Report was based in part on telephone interviews with youth ages 10-17 whose parents or guardians were notified that the interview would discuss "sexual material your child may have seen" and who then gave permission for such interviews. Although the interviewers told the youth their responses would be "confidential," readers should recognize that it is at least possible the pre-teenage and teenage youth who were interviewed, knowing that their parents were aware they were being questioned about their online activity involving sexual material, may have distrusted the confidentiality of the survey and underreported that activity for fear that their parents would learn that they had engaged in certain behavior or practices online of which their parents would disapprove.[2]

The Department disagrees with any implication that the risk online predators pose to children is extremely small. For example, reports of online enticement of children for sexual acts to the National Center for Missing & Exploited Children's CyberTipline increased from 707 in 1998 to 5,759 in 2009. Moreover, documented online enticement complaints processed by ICAC Task Forces, which include both complaints based on undercover operations where agents pose as minors and complaints based on the enticement of actual minors, increased from 3,572 in 2004 to 8,313 in 2008. The information presented in the Education Section should thus be considered in context, given this data.

Because the health and safety of our children is important to us as a society, we devote significant resources to combating these serious crimes through education, by investigating and prosecuting the offenders, and by providing services and restitution to crime victims. These resources are well spent because providing education and training to better protect children and to assist law enforcement in identifying perpetrators, rescuing child victims, and training law enforcement and court personnel to handle these cases more effectively is a critical component in our strategy to prevent child exploitation. Accordingly, while the Department agrees that research will assist in targeting sound prevention messages to the populations those messages will most benefit, and that prevention messages should include teaching social responsibility as a core component of personal safety, the Department believes it important that prevention messages not minimize the risk to children posed by online predators.

The Department will soon be releasing a Report to Congress on The National Strategy for Child Exploitation Prevention and Interdiction ("National Strategy"), as required by the PROTECT Our Children Act of 2008. The Department invites readers to review the National Strategy, which will include a detailed assessment of child exploitation threats, including an assessment of the threat of online enticement.

[1] Of course, points of view or opinions stated in Department-funded research are those of the authors of the research and do not necessarily represent the official position or policies of the Department.
[2] The first CCRC youth telephone survey was conducted between 1999 and 2000, and the second in 2005. Given the rapidly-changing nature of the Internet, readers may wish to consider the age of this research.

ConnectSafely
Smart Socializing Starts Here™

Statement of Anne Collier
Co-Chair
Online Safety and Technology Working Group
Co-Director
ConnectSafely.org **June 4, 2010**

As Hemu and I stated in the Executive Summary to this report, we are indebted to the insightful, collaborative work of our fellow OSTWG members, especially that of our remarkable subcommittee chairs, Chris Bubb, Larry Magid, Mike McKeehan, and Adam Thierer. We can't thank them enough. And I can't thank my co-chair, Hemanshu Nigam, enough for all the experience and hard work he brought to our task.

We are also grateful for the dedicated support of the National Telecommunications and Information Administration. NTIA staff did a lot more than gather and advise the Working Group, and we are thankful to them for many hours of support often well beyond "business hours."

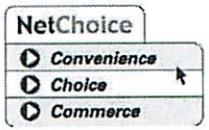
The statute that called for our formation did not ask us to advance the public discussion about youth online safety, but we felt it imperative to do so. In addition to the challenge of responding fully to the statute, we were challenged with the task of building on the fine work of the COPA Commission, the Committee to Study Tools and Strategies for Protecting Kids from Pornography at the National Research Council, the Internet Safety Technical Task Force at Harvard University's Berkman Center, and many other blue-ribbon bodies in the US and other parts of the world.

With the insights from social media scholars, educators, and risk-prevention practitioners represented in this report, I am delighted to say the OSTWG Report does indeed advance the discussion. Our report puts on record the latest thinking on youth online safety, from risk-prevention practitioners' call for application of the public health field's three-tiered prevention model to recognition of the need for a coordinated, multi-disciplinary approach to youth online safety at the federal level.

It's now time to move forward, with targeted, evaluated online risk prevention and intervention by all fields working in child protection; coordinated, multidisciplinary federal government support; a national commitment to pre-K-through-12 instruction in digital media literacy and citizenship; and...

...as we say at ConnectSafety.org, Internet safety set in the positive context of young people's full, constructive engagement in participatory media, culture, and democracy.[i]

[i] "Online Safety 3.0: Empowering and Protecting Youth" (http://os3.connectsafely.org)



Promoting Convenience, Choice, and Commerce on the Net

The NetChoice Coalition
1401 K St NW, Suite 502
Washington, DC 20005
202.420.7482

www.netchoice.org

NetChoice Comments on Final Report of the Online Safety and Technology Working Group

NetChoice is thankful to have participated on the Online Safety and Technology Working Group (OSTWG). During the past year, we have heard from experts on a number of various issues related to child safety on the Internet. This report reflects the thoughtful insights of these experts and the hard work of OSTWG members.

Importantly, the report is the most up-to-date snapshot of the online safety efforts of educators, industry and law enforcement. Overall, it is overwhelmingly positive great strides have been made in understanding the nature of the threat and how to respond:

- Most youth capably deal with Internet problems. Parenting styles are strongly related to online experiences, behaviors and attitudes.
- Harm prevention needs to be tailored to risk, and online risk correlates with offline risk.
- The parental controls technology marketplace continues to evolve rapidly and work best in tandem with educational strategies, parental involvement, and mentoring.

Understanding the true risks of online communications is the first step toward crafting public policy solutions. In this regard, there are important recommendations for policymakers:

- Government should avoid inflexible, top-down technological mandates.
- Media literacy should be a national priority.
- Congress should assess the effectiveness of current data preservation requirements before considering data retention mandates.

The report underscores the privacy and free speech interests of citizens when using Internet communications, and the tensions that exist with law enforcement desire to access data. NetChoice believes that the Electronic Communications Privacy Act (ECPA) should be amended to reflect modern Internet communications. Updating ECPA would go a long way to allow online computer services to better provide and preserve data for law enforcement investigations, while still protecting the constitutional rights of citizens.

But perhaps it is what the report does not include that is of equal importance to Congress and other policymakers. OSTWG specifically considered and rejected a recommendation for online content and service providers to develop parental control technologies according to a common language. The working group recognized the risk that standardization could freeze innovation and make it more difficult for online services to create user interfaces tailored to their products.

Going forward, NetChoice will continue to work with state, federal and international policymakers to implement the report recommendations and further improve online safety for children.

Online Safety Technical Working Group
Brian Cute
Comments

Online safety is a complex, dynamic and fluid challenge for youth, parents, industry, society and the government. My participation on the Online Safety Technical Working Group (OSTWG) has served to confirm this fact. The dynamic nature of the Internet presents something of a moving target when trying to identify the surest, most predictable ways to disseminate useful information concerning safe Internet practices to youth and adults alike. The interaction of all stakeholders is critical and yet no single stakeholder can deliver the silver bullet solution to this challenge. What remains constant is that the school system provides an environment in which online safety practices can be communicated to the youth of America in a structured and meaningful way.

What became painfully obvious in our exploration of online safety in the school setting is that the introduction of Internet safety training through the traditional channels of "curriculum development" and "teacher training" will take too long to equip today's youth with the necessary tools to use the Internet as responsible Digital Citizens. Indeed it will be years before we can answer such questions as "should Internet safety be its own subject matter" or "should Internet safety be developed as adjunct curriculum to computer and IT studies" or "should Internet safety be integrated across all existing curriculum as a 'cross cutting' issue." All the while, our children will be adopting the latest Internet or gaming technologies, blithely exposing themselves to new risks or inadvertently allowing malicious actors to perpetuate nefarious practices through young users' ignorance of basic computer and Internet "hygiene."

The OSTWG Education Subcommittee's recommendation to "Create a Digital Literacy Corps for Schools and Communities Nationwide" should be our most pressing national priority. Finding creative means to get instruction on Internet safety into the school setting today is critical. Programs like AmeriCorps or modifications to existing student grant or loan programs could attract capable college aged students or graduates to deliver Internet safety study into the school setting in the short term. This first wave of Internet safety instruction should be set in motion while structured curriculum development and teacher training processes proceed in parallel. The creation of a Digital Literacy Corps is the first critical step down this all important road.

ARIZONA FAMILY COUNCIL

Prior to the Internet, great efforts were made to protect children from inadvertent and intentional exposure to pornography. Today solid, concrete barriers exist in the physical world such as criminal laws, zoning laws, restrictions on retail establishments, identification verification, etc. to help prevent children from being exposed to pornography. The virtual world, however, provides breakable and in many instances, non-existent barriers to even inadvertent exposure to pornography.

The harm from exposure to pornography is a significant risk children face on the Internet today. It is no longer a question of *if* a child will be exposed to pornography, but *when*. 9 out of 10 children ages 8-16 have viewed Internet pornography, usually unintentionally (London School of Economics, January 2002). A study from Columbia University reports that 75% of boys ages 16-17 *regularly* view and download pornography. Not only is pornography reaching most of the Internet child population, it is having a negative effect. The minimum harm to children from exposure to pornography is poor sex-education and degrading views of women. Some of the more severe harms are sexual crime and addiction. A study of juvenile sex offenders reports that twenty-nine out of thirty offenders had viewed x-rated materials at an average age of seven and a half.

Because children can be severely harmed by exposure to pornographic materials, more needs to be done to:

- educate teachers, parents and children of the potential harms - Internet safety education needs to include information on the addictive nature of pornography;
- build upon the research of the mental, physical, social, emotional, familial and relationship harms of pornography exposure - Responsible government should fund more medical and scientific research on the harms to children from exposure to pornography;
- establish solid, concrete barriers in the virtual world to protect children from these harms through legislative, law enforcement and free-market incentives – families need to be empowered with options to protect their children on the Internet.

Children's exposure to pornography online is just as damaging and threatening as any other online threat because it grooms victims and perpetrators of sexual crimes, introduces children to an illegal and addictive substance, and robs them of an age of innocence worth protecting. Because of the latest medical and scientific research, pornography is not solely a moral issue. It is a public health and societal issue. More needs to be done by government and society to protect children, families, and our communities from the harms of children being exposed to pornography.

Resources:
Media in the lives of 8-18 year-olds http://www.kff.org/entmedia/8010.cfm
"The Social Costs of Pornography" by the Witherspoon Institute
http://www.internetsafety101.org/upload/file/Social%20Costs%20of%20Pornography%20Report.pdf
"The Harms of Pornography Exposure Among Children and Young People" by Michael Flood
http://www.xyonline.net/sites/default/files/Flood,%20The%20harms%20of%20pornography%20exposure%2009.pdf

iKeepSafe

OSTWG Report: Appendix D
iKeepSafe Statement

iKeepsafe would like to thank the OSTWG committee members for their thoughtful contributions to the final report. We anticipate that this effort will help congress as it allocates resources, sets policy, and encourages industry regarding child safety and privacy online.

We encourage all stakeholders (industry, policy leaders, public health, education, law enforcement, parents and youth) to consider how all aspects of an incident might be better handled:

- ***Pre-Incident:*** Prepare for an incident by developing easy-to-use reporting mechanisms that interface with public health and law enforcement. Develop policy, implement prevention/intervention programs, and establish protocol for incident management.
- ***At the time of Incident:*** Implement strategies on how best to respond to the victim, perpetrator, and any bystanders of an incident (i.e., fact finding, documentation, and reporting when necessary).
- ***Post-incident assessment:*** Follow-up with the parties involved. Track outcomes of response, trends, and implement redesign of reporting mechanisms where helpful.

Pre-Incident
Industry can provide more robust family and privacy settings across all platforms, with streamlined connectivity management for parents and reporting mechanisms. We recognize that many providers of Web and mobile products have made noticeable strides to simplify and streamline family settings and reporting mechanisms whereby users and their parents can report inappropriate content, bad behavior/harassment, and terms of service violations. Despite these efforts, most parents remain overwhelmed by the requirements of managing family and privacy settings. Going forward, we encourage industry to voluntarily come together to streamline (where possible) family settings across platforms, so that once a parent has mastered the controls in one platform, he or she can transfer that expertise to other venues. We recognize the need for businesses to differentiate their products and protect their brands, and we are confident that individuation can be maintained while still improving usability and uptake of online safety features in homes. We also encourage industry to offer products with the family settings enabled as default.

At the Time of the Incident
Industry can reach out to bystanders by providing robust ways for them to self-police their communities and to intervene when they see a peer engaging in high-risk/illegal online behavior or harassment (either as victim or perpetrator). Bystanders should be able to quickly respond by reaching public health venues through online mechanisms when they see evidence of suicide or other life threatening situations.

Post-incident
One area where congress can make a significant difference is in providing funding for research and professional development to law enforcement, education and public health communities. We see very little funding to help public health and education communities be more effective and relevant as they respond to youth needs in a digital environment and preparing youth for full digital citizenship.

We are hopeful that as the technologies surrounding connectivity improve, the safety and privacy management features will grow with them towards a more friendly, plug-and-play interface where non-technical users find safety features and content filtering enabled as the default and where problems can be resolved through easy, established channels.

Marsali Hancock, President
Internet Keep Safe Coalition

INTERNET KEEP SAFE COALITION
4607 40th Street North, Arlington, VA 22207-2961 703.536.1637 / www.ikeepsafe.org

StaySafeOnline.org
National Cyber Security Alliance

The National Cyber Security Alliance (NCSA) is **not** submitting a dissenting point of view about this report.

NCSA joined OSTWG assuming that to be a success the final report to Congress would be inclusive of a broad range of viewpoints and not that NCSA would necessarily agree with each and every recommendation in every area the report covers.

The report was developed by active participation of a diverse group of representatives from industry, government, and the nonprofit sector. As it should, the findings and recommendations represent the great breadth and depth of the field. In NCSA's opinion, that's what gives the document credibility.

Moving together in unison is the best way to achieve our shared vision of making the Internet and cyberspace as safe and secure as possible for young people.

verizon

May 21, 2010

Statement Regarding the NTIA Online Safety and Technology Working Group s Final Report to Congress and the Secretary of Commerce

Verizon commends the Working Group for the high quality of its report on the state of Internet safety in the U.S. today. We applaud the fine work and research captured in the report and we agree with most of the recommendations. There are several additional points that Verizon believes Congress and the Administration need to take into account as they consider the current and future state of Internet safety:

- **Regulation would diminish, not improve, Internet safety.** The Internet is a global network of networks. The public Internet is made up of more than 25,000 interconnected networks owned and operated by corporations, governments, schools, and not-for-profits across the globe. Because not all these networks are located in the United States, local attempts to regulate the global Internet are at best ineffective and at worst detrimental to the proper functioning of the Internet. For example, attempts to regulate how network operators manage their networks may have the unintended consequence of tying their hands when it comes to responding the ever-changing real-time threats we see on today s Internet.

- **To the extent legislation or regulation of Internet safety is pursued, it should be only at the federal level.** The Internet is by its very nature an interstate (indeed, international) network. Standards for Internet safety, if they are to be adopted at all, should mirror the broad, cross-jurisdictional nature of the Internet. Conversely, if states were to set their own standards, the resulting patchwork of regulation would impose a confusing burden on the industry -- with as many as 54 different sets of requirements, creating uncertainty for consumers, parents, law enforcement, and industry participants.

- **Congress should take a wait and see approach before acting in the area of Internet safety.** Congress should first assess the impact of the more focused and efficient data preservation procedures enacted in the PROTECT Our Children Act before considering mandatory data retention or other provisions impacting Internet safety. Also, federal agencies have task forces and working groups looking at the efficacy of privacy laws to protect consumers when online and marketing to children online. The conclusions of these efforts need to be factored into any Congressional action on Internet safety.

Verizon takes its responsibility to protect its customers from Internet threats very seriously, just as we have long demonstrated our commitment to protecting customer privacy. We look forward to working with our industry partners to make the Internet a safer place for children, parents, and increasingly, seniors, in a cooperative and collaborative fashion. Verizon looks forward to participating in that dialog.

KEEPING THE INTERNET
OPEN • INNOVATIVE • FREE

www.cdt.org

CENTER FOR DEMOCRACY & TECHNOLOGY

1634 I Street, NW
Suite 1100
Washington, DC 20006

P +1-202-637-9800
F +1-202-637-0968
E info@cdt.org

Statement of **John B. Morris, Jr.**
Center for Democracy & Technology

ONLINE SAFETY TECHNOLOGY WORKING GROUP

May 26, 2010

We commend the OSTWG participants for completing an important analysis of online safety issues, especially in light of the lack of resources available to the group to conduct any serious data gathering. We agree with the broad conclusion that a combination of education and technology tools are the most effective means that parents can use to protect their children online. The work of the OSTWG reinforces the conclusions of past blue ribbon panels that have endorsed education and technology tools.

A primary point of contention within the Working Group centered on the question of data retention – whether service providers should record and retain information about users' Internet use. Unsurprisingly, law enforcement participants support data retention, while civil liberties advocates and industry representatives believe that data retention poses serious privacy concerns. We believe that law enforcement can take advantage of other options for directing service providers to preserve information needed for specific investigations (as opposed to a broad mandate that required that information be retained about all users).

What is surprising, however, is the breadth of data retention sought in this report by law enforcement. The debate thus far over data retention has centered on possible requirements on Internet access providers for them to retain records of "IP address allocations," which could be used to link an e-mail or other online communication to a particular Internet subscriber. Even this type of proposal, which is focused on a narrow set of data retained only by a user's access provider, raises serious privacy and other concerns.

In this report, however, law enforcement is advocating for a radically broader and more invasive approach to data retention, in which any online service on the Internet which allows users to post any content, information, or comment would be required to keep track of every interaction with every visitor to their sites. The reach of this proposal is breathtaking and would require the tracking and storage of a vast amount of information documenting exactly where Internet users go and what they do online. This type of sweeping data retention would transform the Internet from an open forum for free speech to a massive surveillance system in which users would know that every move they make is recorded and potentially reviewable by the government. There are, as detailed in the report, significant policy problems with the sweeping data retention suggested here.

News Corporation

IN SUPPORT OF

Youth Safety on a Living Internet
Report of the Online Safety and Technology Working Group

For the past 20 years I have been focused on the safety, security, and privacy of individuals – as a prosecutor and a corporate executive. During this time, I have had the honor of providing counsel to or serving on different online safety task forces. Through News Corporation alone, I was involved in the Virginia and Washington State Attorneys General Youth Internet Safety Task Forces, the Berkman Center's Internet Safety Technical Task Force, and this OSTWG.

And as News Corporation's Chief Security Officer, I had the privilege of serving a company for whom the safety, security, and privacy of its online users has remained a top priority. On behalf of News Corporation, I congratulate the OSTWG for successfully completing a well-grounded and collaborative effort to evaluate industry efforts to promote a safer online environment for children. We thank the members for their time, effort, and dedication in bringing this report to fruition.

I also want to personally thank Anne Collier. As co-chair of the OSTWG, Anne was a sincere pleasure to partner with. Her dedication, strength of conviction, and safety acumen allowed us to jointly lead a group of experts from every facet of the safety ecosystem towards areas of true agreement and collaboration. During our tenure, we saw incredible leadership from Chris Bubb, Larry Magid, Michael McKeehan, and Adam Thierer, our subcommittee chairs that were given the challenging task of putting the pieces together for each area we focused on – and they did. To them, we offer a heartfelt thank you. Finally, we extend a sincere appreciation to NTIA and especially to Assistant Secretary Lawrence Strickling, Danny Weitzner, Tim Sloan, and Joe Gattuso for the tremendous support this past year.

One recurring theme has become indelible in the last several years – a holistic approach must be taken in order for us to have a significant impact on the online safety of our nation's youth. This report provides recommendations designed to lay the foundations for this holistic approach to prosper today and in the years to come. Simply put, child online safety solutions must be the result of active participation from every stakeholder in society. Only then can we succeed.

Online safety must remain a journey, not a destination.

Hemanshu Nigam
Co-Chair, OSTWG
Safety Advisor, News Corporation (former Chief Security Officer)

USTELECOM
THE BROADBAND ASSOCIATION

United States Telecom Association (USTelecom) Statement Regarding the Online Safety and Technology Working Group (OSTWG) Final Report to Congress

USTelecom thanks the OSTWG Co-Chairs, Hemanshu Nigam and Anne Collier for their leadership over the past year, as well as the individual members of the OSTWG for their joint efforts and individual contributions. As the premier trade association representing service providers and suppliers for the telecommunications industry, USTelecom was honored to be a part of this group and remains committed to ensuring that families and children are safe and secure online. The OSTWG was fortunate to have representatives from nearly every facet of the child online safety ecosystem represented, including the Internet industry, child safety advocacy organizations, educational communities, and the government, and law enforcement communities. Despite the broad range of membership in the OSTWG, there was substantial consensus regarding the current status of online safety efforts.

The OSTWG agreed that no "silver bullet" can address the many facets of youth online safety. Parents, educators, and others are utilizing a broad array of tools that include educational resources, parental control technologies, family and school policies, and government education efforts. USTelecom agrees with the OSTWG's assessment that "any solution to online safety must be holistic in nature and multi-dimensional in breadth." Many of USTelecom's members are at the forefront of providing consumers with the tools they need to ensure that families and children have a safe and secure online experience.

USTelecom's member companies also remain dedicated to the fight against child exploitation on the Internet. We applaud the efforts of our partners in this effort, including the National Center for Missing and Exploited Children (NCMEC) and the law enforcement community. Thanks in part to these ongoing collaborative efforts, recent changes to Federal law, the recommendations contained in the report, USTelecom is optimistic that these factors will help accelerate investigative efforts and spur additional criminal prosecutions of child pornography offenders.

While the report noted the contentious aspect of data retention, USTelecom supports the subcommittee's ultimate recommendations, including increased communication between law enforcement and network providers. Moving forward, we look forward to active dialog with our law enforcement partners and other stakeholders to achieve similar goals. USTelecom believes such active dialogue will result in achieving the appropriate balance between the legitimate needs of law enforcement, consumers' rightful privacy concerns, and the valid operational and business concerns of network providers.

USTelecom is committed to fulfilling the OSTWG's recommendation to "fill the prescription." Our member companies take very seriously their shared responsibility to keep families and children safe and secure in the online environment. We look forward to continuing our work with government, industry and non-profit partners to improve upon the practices and offerings to make the Internet a safer place for families and children.

607 14th Street NW, Suite 400 • Washington, DC 20005-2164 • 202.326.7300 T • 202.326.7333 F • www.ustelecom.org

NATIONAL CENTER FOR MISSING & EXPLOITED CHILDREN

The National Center for Missing & Exploited Children (NCMEC) is grateful for the opportunity to participate in the Online Safety and Technology Working Group (OSTWG). The OSTWG Members represent a wide range of key constituencies and perspectives on these issues. The diversity of the Members resulted in lively and productive exchanges on such topics as Internet safety education, sexting, data retention, safety tools and industry efforts regarding sexually abusive images of children.

We thank Anne Collier and Hemanshu Nigam for their leadership, the subcommittee chairs and all the Members for dedicating their time and effort to this report.

NCMEC recognizes that procedural limitations on the OSTWG subcommittees, specifically their inability to conduct surveys or new research, hindered their work. The OSTWG subcommittees would have likely been able to achieve a more complete understanding of the issues and subsequently provide more robust recommendations if they had been able to conduct surveys. Instead, the group had to rely on research that is more than 5 years old and has already been reviewed by a prior task group (the Internet Safety Technical Task Force). This report would have benefitted significantly from more current research on the issues, whether conducted by OSTWG or other groups. Technology, and how people use it changes rapidly, which reinforces the critical need for up-to-date research on these issues. Policymakers should consider only the most recent data in drafting solutions to Internet-facilitated problems.

NCMEC is troubled by the report's emphasis on the prevalence of peer-on-peer predation. We are concerned that this focus seems to discount the threat of adult predation and the impact that peer-on-peer predation has on child victims. Regardless of the source of the predation, any unwanted sexual solicitation should be treated as a serious problem by parents/guardians, Internet safety advocates and policymakers. We urge policymakers to treat online peer-on-peer predation with the same degree of concern as cyberbullying, another type of malicious peer-on-peer conduct.

In addition, while children are being enticed online by other children, it is important not to diminish the fact that children are being enticed into sexual activity by adults in significant numbers. Reports to NCMEC's CyberTipline regarding enticement have increased 714% since 1998. There is an urgent need for current research on this issue. We urge policymakers to seek out a range of sources, including industry and law enforcement, to quantify the scope of this problem.

OSTWG covered a wide range of issues and, in many areas, has provided strong recommendations for consideration. We applaud the Members for their efforts and commitment. The limitation of NCMEC's comments to these discrete issues should not be considered to be an endorsement of the report in its entirety.

CTIA Commends the National Telecommunications & Information Administration's Working Group Report on Online Safety Tools and Initiatives

CTIA – The Wireless Association®[1] commends the U.S. Department of Commerce National Telecommunications & Information Administration's ("NTIA") Online Safety & Technology Working Group ("OSTWG") for their efforts in outlining the communications industry's initiatives to promote responsible online use among children and teens. While the OSTWG report describes the inappropriate and irresponsible ways children and teens may be using online technology, including texting while driving, sexting, and cyberbullying, CTIA believes the report demonstrates the wireless industry's commitment to offer tools that are providing parents with choice and control over the content and services their children utilize. The OSTWG report also highlights industry's efforts to support law enforcement in the eradication of child pornography, and cooperate with lawful requests for information from law enforcement while protecting consumer privacy and constitutional rights.

Through a diverse wireless ecosystem of service providers, device manufacturers, and software and application developers, the wireless industry is proactively facilitating the educational and social growth of today's youth by preparing them for an increasingly digitized and mobile future. Today, mobile technology offers many educational benefits to children and teens, including mLearning and thousands of educational "apps" focused on language and literacy programs, news, and in-class teaching opportunities.[2]

CTIA and the wireless industry are taking steps to educate kids, parents and teachers about responsible wireless use in these evolving mobile environments. For example, CTIA and The Wireless Foundation recently announced *Be Smart. Be Fair. Be Safe: Responsible Wireless Use* (http://www.besmartwireless.com/), a national education campaign focused on equipping parents and caregivers with the necessary materials and tools to help kids use their wireless devices responsibly. In addition, CTIA has developed a number of voluntary best practices and guidelines under which carriers and manufacturers agree to provide significant protections for consumers and, most specifically, children. In April 2010, CTIA released an update of the wireless industry's voluntary "Best Practices and Guidelines for Location-Based Services," which promotes and protects the privacy of wireless customers' location information.[3]

The wireless industry has proactively deployed effective tools that empower parents, and it will continue to innovate in the future. As the wireless industry develops innovative devices, cutting-edge applications and deploys next-generation networks, CTIA believes that our industry's best practices must continue to evolve to reflect the growing consumer demands in the wireless ecosystem. It is our hope that the NTIA report will help to inform online safety initiatives at the federal, state and local levels of government and further encourage partnerships with the wireless industry to educate America's youth about responsible wireless use.

[1] CTIA – The Wireless Association® (www.ctia.org) is the international association for the wireless telecommunications industry, representing carriers, manufacturers and wireless Internet providers.

[2] Comments of CTIA-The Wireless Association, FCC, MB Docket No. 09-194 (February 24, 2010), *available at* http://fjallfoss.fcc.gov/ecfs/document/view?id=7020390790.

[3] CTIA, Business Resources, Wireless Internet Caucus, *Best Practices and Guidelines for Location Based Services*, http://www.ctia.org/business_resources/wic/index.cfm/AID/11300 (last visited May 18, 2010).

Adam Thierer
President,
The Progress & Freedom Foundation (www.PFF.org)

THE PROGRESS & FREEDOM FOUNDATION

It has been a privilege to serve on this working group and to direct its subcommittee on parental control technologies. I greatly appreciate being given this opportunity, and it was a joy to work with so many brilliant experts, advocates, academics, and industry leaders who were uniformly dedicated to making our children's online experiences safer and more satisfying.

Consistent with what other blue ribbon working groups, task forces, and various experts have found many times before, OSTWG members have generally concluded that there is no silver-bullet technical solution to online child safety concerns. Instead – and again in agreement with previous research and reports – we have concluded that a diverse toolbox must be brought to bear on these problems and concerns. In essence, we have generally endorsed what I have elsewhere referred to as the "3-E" solution, which stands for Education, Empowerment, and Enforcement:

- *Education and mentoring* is the most essential part of the solution. We can—and must—do more as parents and as a society to guide our children's behavior and choices online.
- *Empowerment* is also essential, however. We can provide parents with more and better tools to make informed decisions about media and communications tools in their lives and the lives of their children. But technical tools can only supplement—they can never supplant—education, parental guidance, and better mentoring.
- *Enforcement* of laws and policies is also essential. We need to make sure that law enforcement officials have the resources they need to carry out the important task of protecting children from legitimate online threats.

The OSTWG task force report puts meat on the bones of this "3-E" model and provides the public and policymakers with a wealth of sound advice regarding the steps that should be taken to ensure our kids have safer online experiences.

Importantly, we have accomplished this without resorting to the "moral panic" tone that some have adopted when approaching these issues and concerns. While there are serious challenges and concerns surrounding discussions about child safety, it's important to acknowledge the important benefits of new media and communications technologies to us and our children. We have done so here.

Moreover, we have been careful not to try to unsettle any settled First Amendment law. One of the most regrettable developments of the past 15 years is that so much time has been wasted passing and then litigating legislative and regulatory enactments that have been so clearly unconstitutional under the First Amendment. If the time and resources that were squandered in those legal skirmishes would have instead been plowed into education, empowerment, and enforcement-based efforts, it could have made a lasting difference. More generally, we should always remember the sage advice offered by the Supreme Court in 2000: "Technology expands the capacity to choose; and it denies the potential of this revolution if we assume the Government is best positioned to make these choices for us."

We have charted a sensible way forward in this report that should hopefully avoid those problems. It is my hope that policymakers take our findings and recommendations seriously and adopt the sort of constructive, practical approach we have outlined here.

Evolve the Internet to Protect Families

CP80.org and ThinkAtomic appreciate the opportunity to serve on OSTWG and thank the other members, especially the co-chairs and subcommittee chairs, for their contributions and hard work. While there are many conclusions in the OSTWG Report with which we agree, especially those urging greater education of parents and children, additional factors should be taken into account by Congress and the Administration. Specific mention of certain issues in this Addendum should not be taken to mean that we necessarily agree with any other aspects of the Report.

The primary problem with the OSTWG effort is we were unable to conduct surveys or other data gathering. Especially in the parental controls subcommittee, we did none of our own research and did little to incorporate existing data to support the generalizations and opinions of OSTWG members. For instance, we heard descriptions of various products promoted by the industry, but we made no attempt to do a complete review of what is and is not available, and we made no findings on the effectiveness of any parental control device or program. This kind of analysis was, however, recently conducted by the Berkman Center for Internet and Society. Because OSTWG was unable to conduct our own evaluations, the findings of this study provide better information on parental controls.

We agree there is no "silver bullet" solution, but parents deserve an effective blocking option for protecting children online. While a broad variety of tools are indeed available, we believe this report overstates their effectiveness and avoids the frank truth about the problems of each kind of tool. Moreover, the increasing use of "proxy" sites, the ready availability of filter-circumventing advice (as on Wikipedia), and especially the onset of "cloud" services have nullified parental efforts. Something is clearly not working when only a little over "half (54 %) of internet-connected families with teens now use filters." Especially disconcerting is the ability of minors to access unfiltered Internet with mobile devices almost everywhere. "[E]ffective filtering systems [are not] widely in place on cell phones with internet access or iPods . . . , despite the popularity of such contemporary media among adolescents."

Parents deserve the support of government in making decisions about the education of their children. The laws in place in the real world to protect children largely do not apply online, and where the law does apply, such as the prohibition on obscenity and child porn, law enforcement are given insufficient resources to keep up. Government needs to do more than wait and see, conduct studies, and educate children on avoiding harm. Illegal activity on the Internet needs to be stopped. Certainly, we are entitled to minimum data retention requirements similar to those for telephone records and drivers and vehicle licensing.

While the industry recognizes protecting minors is a "high priority," greater scrutiny needs to be focused on exactly what measures are being taken to assure results, especially, as the Report acknowledges, now that the industry heeds calls for even greater lack of accountability in the name of privacy.

Ralph Yarro III
Chairman, Board of Trustees
The CP80 Foundation

Technology

"We have to do everything we can to encourage the entrepreneurial spirit, wherever we find it. We should be helping American companies compete and sell their products all over the world. We should be making it easier and faster to turn new ideas into new jobs and new businesses. And we should knock down any barriers that stand in the way. Because if we're going to create jobs now and in the future, we're going to have to out-build and out-educate and out-innovate every other country on Earth."

-PRESIDENT BARACK OBAMA, SEPTEMBER 16, 2011

Guiding Principles

President Obama recognizes that technology is an essential ingredient of economic growth and job creation. Ensuring America has 21st century digital infrastructure—such as high-speed broadband Internet access, fourth-generation (4G) wireless networks, new health care information technology and a modernized electrical grid—is critical to our long-term prosperity and competitiveness.

The President is committed to ensuring America has a thriving and growing

Internet economy. The Internet has become a global platform for communication, commerce and individual expression, and now promises to support breakthroughs in important national priorities such as health care, education and energy. Additionally, the Internet and information technology can be applied to make government more effective, transparent and accessible to all Americans.

Examples of Progress

1. Cybersecurity and Internet Policy
2. A Modernized Patent System
3. Bringing Technology from "Lab to Market"
4. 21st Century Digital Infrastructure
5. Creating an Open and Accountable Government
6. Learning Technologies
7. Advanced Manufacturing
8. Robotics
9. Federal Chief Information Officers
0. Open Data Initiatives
1. Presidential Innovation Fellows
2. First U.S. Chief Technology Officer

Cybersecurity and Internet Policy

President Obama has pledged to preserve the free and open nature of the Internet to encourage innovation, protect consumer choice, and defend free speech. The Administration has created an Internet Policy Task Force to bring together industry, consumer groups, and policy experts to identify ways of ensuring that the Internet remains a reliable and trustworthy resource for consumers and businesses.

In July 2011, at the Organisation for Economic Co-operation and Development (OECD), the Obama Administration joined with representatives from business, civil society, and Internet technical communities from 34 countries to reaffirm the importance of Internet policy principles that have enabled the open Internet to flourish with innovation and human connections beyond our wildest expectations.

Americans deserve an Internet that is safe and secure, so they can shop, bank, communicate, and learn online without fear their accounts will be hacked or their identity stolen. President Obama has declared that the "cyber threat is one of the most serious economic and national security challenges we face as a nation" and that "America's economic prosperity in the 21st century will depend on cybersecurity." To help the country meet this challenge and to ensure the Internet can continue as an engine of growth and prosperity, the Administration is implementing the National Strategy for Trusted Identities in Cyberspace. The

Administration also released the International Strategy for Cyberspace to promote the free flow of information, the security and privacy of data, and the integrity of the interconnected networks, which are all essential to American and global economic prosperity and security.

President Obama has responded to Congress' call for input on the cybersecurity legislation that our Nation needs, and the Administration will continue to engage with Congress as it moves forward.

The Obama Administration has also prioritized the cybersecurity of federal departments and agencies. In addition, the Administration has matured the government's implementation of the Federal Information Security Management Act (FISMA) away from a static, paper-based process to a dynamic, relevant process based upon continuous monitoring and risk assessment.

A Modernized Patent System

President Obama signed the *America Invents Act* into law on September 16, 2011 after nearly a decade of effort to reform the Nation's outdated patent laws. The patent reform law helps companies and inventors avoid costly delays and unnecessary litigation—letting them focus instead on innovation and job creation. Many key industries in which the United States leads, such as biotechnology, medical devices, telecommunications, the Internet, and advanced manufacturing, depend on a strong and healthy intellectual property system.

The law has a number of transformative initiatives that build on reforms already underway under the leadership of the U.S. Patent and Trademark Office Director David Kappos. The law gives the USPTO the resources to reduce patent application waiting times significantly, and builds on the great strides the patent office has already made, reducing its backlog by 15% during this Administration even as the number of filings per year has increased. The USPTO has also launched an accelerated examination program, known as Track One, that allows patent applications to be processed to completion in 12 months and offers small businesses a 50 percent discount on this option.

Under Track One, the USPTO has offered 3,502 companies, and over 1,278 small businesses the opportunity to move their technologies to the marketplace faster—accelerating the creation of new jobs and new industries. In the only 7 months since the program has started, we've issued a total of 101 completed patents through the program, with applicants waiting only about an average 117.3 days to receive a complete decision on their application. The program builds on the Green Technology Pilot program that accelerated 3,500 patent applications involving reduced greenhouse gas emissions and energy conservation — at no cost to the inventor. USPTO has also recently launched the Patents for Humanity pilot program, which creates business incentives for patent holders to engage in humanitarian issues.

Excessive litigation has also long plagued the patent system. The *America*

Invents Act offers entrepreneurs new ways to avoid litigation regarding patent validity, without the expense of going to U.S. District Court, and will also give the USPTO new tools and resources to improve patent quality. In addition to these new tools, the USPTO is also hiring 100 new judges to adjudicate cases in front of the Board of Patent Appeals and Interferences, helping to decrease the backlog of patent appeals cases, and reduce wait times for appellants. The new law also will harmonize the American patent process with the rest of the world to make it more efficient and predictable, and make it easier for entrepreneurs to market products simultaneously in the United States and for exporting abroad.

Bringing Technology from "Lab to Market"

Leading up to the President's signing of the *America Invents Act*, the Administration worked with Federal agencies and private-sector partners to launch a series of new "Lab to Market" initiatives. The initiatives are aimed at helping to achieve the President's goal of strengthening "commercialization of the nearly $148 billion in annual federally-funded research and development", as first proposed in January 2011 at the launch of the White House-led *Startup America* campaign. These efforts encouraged Federal agencies to streamline their technology-transfer procedures, support additional government-industry collaboration, and encourage the commercialization of novel technologies flowing from our Federal laboratories.

21st Century Digital Infrastructure

Wireless Infrastructure: President Obama's National Wireless Initiative will make high-speed wireless services available to at least 98 percent of Americans. The availability of new wireless broadband services will allow more Americans to use the Internet to learn, work and play—regardless of where they live. One aspect of the President's plan is to make more airwaves available (in scientific terms, some 500 Mhz of spectrum), to be available for enhanced cell phones and other wireless services—including dedicated public safety networks—over the next ten years. The President's plan also supports advances in security, reliability and other critical features by investing in research and development in wireless technology. And through the auctioning of airwave space to companies that will develop the next generation of wireless services, the initiative will further R&D investments and deliver an estimated $10 billion for deficit reduction.

Broadband: High-speed internet infrastructure is key to a 21st century information economy. Through $7 billion in targeted investments from the Recovery Act, the Administration has expanded broadband access nationwide, improved high-speed connectivity in rural areas and public computer centers, and increased Internet capacity in schools, libraries, public safety offices, and other community buildings.

A Smarter Power Grid: A 21st century electric system is essential to America's ability to lead the world and create jobs in the clean-energy economy of the

future. As part of the Recovery Act, this Administration invested $4.5 billion in electricity delivery and energy reliability modernization, with total public-private investment amounting to over $10 billion To ensure that all Americans benefit from these smart grid investments, the Administration released a policy framework and a series of new initiatives in June 2011 that will empower consumers with tools to better manage their electricity and cut costs, improve the reliability of the electric grid, and help utilities recover from natural disasters faster. A first generation of innovative consumer products and services—such as thermostats that can be controlled from a smart phone, or websites that show how much energy a house is using—are already helping Americans save money on their electricity bills.

Creating an Open and Accountable Government

Government is more accountable when it is transparent. That's why President Obama signed the Memorandum on Transparency and Open Government on his first full day in office, ushering in a new era of open and accountable government to bridge the gap between the American people and their government. The Administration has taken unprecedented steps to make government more efficient and effective, including the following actions:

- Launched in May 2009, Data.gov has increased access to information that the public can readily find and use. The purpose of Data.gov and Data.gov communities is to increase public access to data and information generated by departments and agencies in the Federal government. For example, you can find monthly data on U.S. oil refinery utilization and capacity back to 1985 or value of mineral production by state. With more than 385,000 such datasets currently online, and more coming all the time, the Administration is continuing to create a more participatory government by expanding access and encouraging creative ways for data to be used.
- Through the U.S.-India Open Government Dialogue, the two countries have partnered to release "Data.gov-in-a-Box," an open source version of the United States' "Data.gov" data portal and India's "India.gov.in" document portal. It will be available for implementation by countries globally, encouraging governments around the world to stand up open data sites that promote transparency, improve citizen engagement, and engage application developers in continuously improving these efforts.
- The Administration has increased tracking of how government uses Federal dollars with easy-to-understand websites like Recovery.gov, USASpending.gov, and the IT Dashboard.
- The Administration is spurring innovation by using challenges and prizes to motivate greater citizen participation in the quest to meet national challenges. In September 2010, the Administration launched Challenge.gov, a one-stop shop where entrepreneurs and citizen solvers can find public-sector prizes. Prizes are a great way to inspire a wide range of potential problem solvers to take aim at problems through innovation. Unlike the case with many conventional grants, the method for achieving success is not narrowly defined and the government pays only

for results. For example, the Department of Defense sponsored a challenge aimed at stopping uncooperative fleeing vehicles without causing permanent damage to the vehicle or its occupants, and got a winning solution from someone who might otherwise never have appeared on that department's grant-making radar.

- In June 2011 President Obama issued an executive order to cut waste, streamline Government operations, and reinforce the performance and management reform gains the Obama Administration has achieved.
- In July 2011 the Obama Administration announced the launch of the Government Accountability and Transparency Board. The Board, first announced by the President and Vice President in June as part of the Campaign to Cut Waste, will focus on rooting out misspent tax dollars and making government spending more accessible and transparent for the American people.
- The National Science and Technology Council (NSTC) Task Force on Smart Disclosure is working to promote better disclosure policies and aid in the timely release of complex information in standardized, machine-readable formats that enable consumers to make informed decisions in numerous domains.
- The White House launched *We the People*, a new platform that gives all Americans a way to create and sign petitions on a range of issues affecting our nation. And if a petition gathers enough online signatures, it will be reviewed by policy experts and you'll receive an official response.
- In September 2011, President Obama and President Rousseff of Brazil hosted the formal launch of the Open Government Partnership (OGP) at an event with Heads of State and senior officials from 46 countries. This meeting focused attention on the shared challenge of improving governance, and demonstrated a strong political commitment around the world to the kinds of reforms necessary to enhance transparency, fight corruption, and strengthen mechanisms of democratic accountability.

Learning Technologies

Technology can be a powerful tool when it comes to teaching and learning. To help realize its potential, in September 2011 the Department of Education and private foundations launched Digital Promise, a new national center for advancing learning technologies. Digital Promise will harness the efforts of everyone from educators to entrepreneurs to spur the research, development, and adoption of breakthrough technologies that can help transform the way teachers teach and students learn. Learn more here.

Advanced Manufacturing

In June, 2011, President Obama launched the Advanced Manufacturing Partnership (AMP), a national effort that brings together industry, universities, and the Federal government to invest in the emerging technologies that will create high-quality manufacturing jobs and enhance our global competitiveness. To launch the AMP, the President announced $300 million of government-wide

investment in domestic manufacturing capabilities, $100 million in research and training investments to develop and deploy advanced materials, $70 million in robotics research and development, and $120 million of investment in innovative energy-efficient manufacturing processes.

The AMP is based on a recommendation of the President's Council of Advisors on Science and Technology (PCAST) in its report "Ensuring Leadership in Advanced Manufacturing." The AMP is led by Andrew Liveris, Chairman, President, and CEO of Dow Chemical, and Susan Hockfield, President of the Massachusetts Institute of Technology.

For more information: President Obama Launches Advanced Manufacturing Partnership

Manufacturing Innovation

On August 16, 2012 in Youngstown, OH, National Economic Advisor Sperling, Acting Secretary of Commerce Rebecca Blank and Under Secretary of Defense Frank Kendall announced the establishment of an additive manufacturing pilot institute by a consortium that includes more than 40 firms, five research universities, and seven community colleges, led by the National Center for Defense Manufacturing and Machining. The pilot institute, which the President announced in his speech at Petersburg, VA on March 9, 2012, will serve as a proof of concept for the proposed National Network for Manufacturing Innovation, currently under Congressional consideration. Up to fifteen Institutes for Manufacturing Innovation are proposed for development in the network. These institutes will serve as regional hubs of manufacturing excellence that will help make U.S. manufacturers more competitive and encourage investment in the United States.

Robotics

President Obama's National Robotics Initiative is part of a broader effort to promote a renaissance of American manufacturing through the Advanced Manufacturing Partnership.

This initiative focuses on developing robots that work with or beside people to extend or augment human capabilities, taking advantage of the different strengths of humans and robots. In addition to investing in the core technology needed for next-generation robotics, the initiative will support applications such as robots that can:

- Increase the productivity of workers in the manufacturing sector;
- Assist astronauts in dangerous and expensive missions;
- Help scientists accelerate the discovery of new, life-saving drugs; and
- Improve food safety by rapidly sensing microbial contamination.

As part of this initiative, the National Science Foundation, the National Institutes of Health, NASA, and the Department of Agriculture are funding $70 million of research for next-generation robotics.

For more information: Developing the Next Generation of Robots

Federal Chief Information Officers

In this 21st century Information Age, virtually all big businesses find it essential to have a Chief Information Officer (CIO)—someone who specializes in making sure that information is flowing smoothly within the business's various components and also between the business and its customers and suppliers. Early in his Administration, President Obama made the important recognition that government, too, could benefit from having a CIO, and he appointed the first in the Federal government's history. (A number of departments and agencies have since appointed CIOs as well.) One of the bigger responsibilities for the Federal CIO has been to find new efficiencies relating to the many information technology projects going on in the government—projects that stand to save taxpayers dollars and make government services more efficient, but which need to be coordinated with one another to achieve these goals.

Toward that end, on December 2010, the Administration released a 25-Point Implementation Plan to reform the way the Federal government manages information technology projects. Office of Management and Budget Director Jack Lew followed up on that Plan in August by issuing a CIO Authorities Memo, which spells out in detail how the CIOs in various departments and agencies should go beyond mere management of information technology projects and focus in addition on making sure they get the highest return on investments in information technology; being transparent and accountable for the status of projects on Federal websites such as the IT Dashboard; and ensuring the security of electronic information.

Part of being efficient involves shutting down projects that are no longer performing, and one responsibility of the Federal CIO and his office has been to use so-called TechStat sessions to look into such projects and figure out how to either fix them or terminate them. The Administration has said it intends to terminate or turn around at least one-third of all underperforming information technology projects by June 2012. The Federal CIO is also working to consolidate Federal data centers and move more and more information from individual computers and physical data centers to "the digital cloud"— part of a cloud-first strategy that promises big gains in efficiency. Finally, CIOs must ensure we are continuously improving our efforts to safeguard Federal data through cybersecurity.

The Federal Chief Information Officer, Steven VanRoekel, highlighted the ways in which he envisions his office fulfilling these goals and is using technology.performance.gov to share our progress effectively managing large-scale IT projects, achieving operational efficiencies, and improving

cybersecurity with the American people.

For more information on the Obama Administration's technology priorities, check out the White House Office of Science and Technology Policy website.

Open Data Initiatives

Under the leadership of the U.S. Chief Technology Officer, the Administration is pursuing initiatives that seek to "liberate" government data and voluntarily-contributed corporate data as fuel to spur entrepreneurship, create value, and create jobs. As a model, decades ago, the National Oceanic and Atmospheric Administration began making weather data available for free electronic download by anyone. Entrepreneurs utilized these data to create weather newscasts, websites, mobile applications, insurance, and much more—generating billions of dollars in annual economic value. Similarly, the government's decision to make the Global Positioning System (GPS) freely available has fueled a vast array of private-sector innovations ranging from navigation systems to precision crop farming, creating huge public benefit and tens of billions of dollars of economic value annually.

We believe there is enormous potential to replicate and expand upon these successes in targeted areas of high impact. Think of vast reservoirs of data, sitting in the vaults of government and industry, as a still largely underutilized national resource that can be injected into the economy—fueling a rising tide of entrepreneurial innovation that can improve Americans' lives in many tangible ways, advance key national priorities in sectors ranging from health to energy to education and more, and contribute significantly to economic growth and job creation.

Building upon what we have learned in executing the highly successful Health Data Initiative over the last two years, we have now launched similar open-data initiatives in the energy, education, and public safety sectors, with additional initiatives in the works.

Presidential Innovation Fellows

In August 2012, U.S. Chief Technology Officer Todd Park and U.S. Chief Information Officer Steven VanRoekel launched the first class of Presidential Innovation Fellows. Selected from a nationwide applicant pool of nearly 700 innovators, the 18 Fellows have agreed to spend six months in Washington to work on five high-impact projects aimed at supporting entrepreneurs, small businesses and the economy, while significantly improving how the Federal Government serves the American people.

The five projects were selected because they are tough but tractable challenges whose solutions could provide immediate benefits and cost-savings to American citizens, entrepreneurs and businesses:

- The Open Data Initiatives – inspired by the massive private sector

innovation catalyzed by the release of government weather and GPS data – will accelerate and expand Administration efforts to make government data more publicly accessible in "computer-readable" form and spur the use of those data by entrepreneurs as fuel for the creation of new products, services, and jobs.

- RFP-EZ aims to develop an online marketplace that will make it easier for the government to do business with small high-growth tech companies, and enabling the government to buy better, lower-cost tech solutions from the full range of American businesses.
- MyGov will create a prototype of a streamlined online system enabling citizens to easily access the information and services from across the Federal Government.
- The 20% Initiative will work to transition "the last mile" of international development assistance payments from cash to electronic methods – lowering administrative costs, promoting financial inclusion, and reducing theft, fraud, and violence.
- Blue Button for America will spread the ability for millions of Americans to easily and securely download their own health information electronically, all while fueling the emergence of time and money saving products and businesses.

The first class of 18 Presidential Innovation Fellows were chosen on the basis of individuals' skill sets and their relevance to the chosen challenges. In addition to the Fellows, the broader public is invited to sign up to follow and contribute to the success of these projects. The Presidential Innovation Fellows program's focus is collaborative problem solving by cross-sector teams of innovators who can rapidly prototype and test solutions in an iterative way until success is achieved.

First U.S. Chief Technology Officer

President Obama created the position of U.S. Chief Technology Officer on his first day in office, noting that corporate leaders have long recognized the value of having a person responsible for ensuring that technology is being used as effectively as possible to advance key objectives. The U.S. CTO is responsible for ensuring and advancing the use of innovative technological approaches to support Administration priorities, including job creation, broader access to affordable health care, enhanced energy efficiency, a more open government, and national and homeland security.

Current U.S. CTO Todd Park is leading an array of efforts, including the Open Data Initiatives and Presidential Innovation Fellows programs, that aim to help modernize a Federal government relying too heavily on 20th century technology, and better leverage the power of technology and data to help address a wide range of national challenges. These initiatives employ an agile, "lean startup"-style approach to effecting change in government, and embrace the idea of collaboration with innovators across the public, private, nonprofit, and academic sectors to deliver the best possible results for the American people.

STS.0858 Lecte 2 9/13

Congress shall make no law, abridging the Freedom
Of Speach, or of the press
- Amendment 1

Hi! Details from Reno
2: John Morris
- laid out the facts

ACLU vs Reno

Getting comments on brief
Whats not written ....
1st interet case
Jim Osbore
Jim Exon - Author of Communications Decency Act

(2)

designed to protect children

Nebraska Football game - w/ Jim Osborne

kids starting to use Interet

kids finding indecent material

Why not make a law?

Congress had always regulated communications

indecent = more than indecent

Pacifica established

7 dirty words

Could just extend rules to the interet

But different

not limited

Commercial + non commercial.

required affirmative action

(3)

All rules not created equally + communications mediums

Speech types

~~[illegible]~~

- town square
  - fund. thing Court tries to protect
  - can walk away ∈ means of control
  - can't force anyone to listen

- print
  - most free
  - Control: don't buy or read!

- they thought it might not be easy to walk away or not read it

(4)

They were thinking broadcast

broadcast

- limited ~~restrictions~~ space
  - use scare comm opportunities in public interest
- easier to ignore
  - turn on TV and see something
  - pervasiveness
    - lots of TV + Radio

- the guy was from Morality + Media
  - he set it up - for certain set of facts
  - was pre arranged
  - both thought they would win
  - for some reason could not turn it off

- also access to opportunity to speak
  - townsquare → free
  - print → could buy - not much $
  - broadcast → public interest
    - so diversity of interests

5

telecom

not as firm as other mediums

Sable - dial - a - porn

900 #s

a somewhat successful

Some more control

no suprise + control

needed to call - affirmative step

CDA amended this section

Court even in tradional services

- no stumbling on objectionable content

Could have gone age verifications

interactive

Created a whole new category

(6)

Whole new medium of expression

parents had mechanisms to control

abundance of speech opportunities

perhaps even more free than print

↑ realized gov goals behind 1st amendment

(seems like we were very lucky on this
but in retrospect obvious
break through old things)

CDA contained clause about how it would be litigated

Congress knew a lot would thrown out

Easier to pass unconstitutional laws

So put this clause in - had decency to that

Congress has a lot of authority on
what courts can rule

7

indecent removed

and patently offensive

transmission display make available

Renton case Zoning of adult theater

majority - this type of censorship not needed at all/ parents could make choices w/ filtering

the 2 - wanted to make sure zoning laws were not undermined
- also road map for Congress

a losing rule may come back later

So is important to offer it

tempting to look at broadcast as an anomaly

but remains a big part of first amendment law

(8)

1st amendment → 1st priority make as much info available to people as possible

Also that global medium - that was new
- State can't really totally control

Indecent exposure
police power
actions not expressions
dress code is more of expression

Cable TV much more permissive
Wardrobe malfunction on cable TV
would prob not be issue

Medium is important
90% of broadcaster watches over cable
is TV even core?
FCC is asking courts to also maintain artificial distinction

(9)

Billboards

local law needed
he's not sure

Jon Maris

Fact guy
1 sr guy + 2 junior guys
Worked w/ experts in internet engineering

Law school clerks were taking internet training at the time

Q n A

Software Systems Designer
Human Rights School
Gener + Black

(10)

RFC author

Alan's mentor

Back in time

Presentation of Fact

2 litigations - got merged

ACLU 1st

focused on valuable speech supressed

like the sexual health network

Was added to much bigger bill

84 - 16 Senate

Politics

People didn't understand how Internet works

Hewing record to back that up

(11)

but didn't really port interet up front

2nd Case

put Interet front + center

Was lenghy

Wash Po i wonky

today everyone knows

- hyperlink

get internet cos to become named plentiful

Cos wouldn't dream about that now

They thought huge threat at the time

Gov

~~Time~~ Pushed Broadcast → Pacifica

Simplistic argument

Screen w/ moving images!

So drew difference

(12)

Scarcity of broadcast
esp w/ digital

also this idea of assult
knowingly go to

My avi banner ads, pop ups
became series of cases COPA
pop ups were not a problem in '97
1999~2000 i unexpected popups had immerged
always worried would come up in COPA
but gov never tried

Why was this difficult in 1996
So radically different than today
Some judges was on email

(13)

Some court didn't have access

Didn't want to demonstrate over 96 kbs

Bell Atlantic installed a T1 line

Brought internet to court

Walked court through surfing

└ demonstrate

Someone really connected w/ the judges

Q What did you show

News site - safe + easy

Discussion boards

list-serv was a brand name

didn't want mailing list

- link / bulk providers

people couldn't send to it

(14)

Said CDA applied to mailing lists
No way for sender to know all identies on list

District court set very solid factual conclusions
- Supreme Court does not ~~rely on~~ look on facts
- Then they just look at law

Other side failed on facts

Asked if could get case online
released electronic version at same time at paper
Uploaded it on a laptop on steps of court
1st decision online within ~10 min
reformatted AOL floppy

(15)

Q: What it today?

have to use - pervasive

Can blah

accidental exposure
- possibly
- not really a problem

he thinks same

tech has advanced

User empowerment Sw

focus was protecting younger miors from accidental minors

could argue gov has little interest in protecting 17 yos from porn

User empowerment tools

not bulletproof

16

Jurisdiction

not really case

'international' was critical later on

So much content is non-US

So rules would not ~~add~~ effect

~~Effect~~

other tools not only least restrictive

but more effective!

Undermines ga interest

Unrest in Middle East from video

which is legal

in part because of Reno

17

He testified before Congress about terrorism recruitment videos

He is a 1st amendment lawyer - protects unpleasant things

Cyberspace is very malleable

This could easily have ended otherwise

But it comes down to people

(18) Cyber Bullying

What should we argue:

not strictly correct → fool proof

What do we want

Goal: improvement in current state of affairs

~~More compelling to~~

Who will support + oppose

3 policy initiatives

Self empowerment

Advocay of parental awaress

1. awareness

2. ~~Awareness~~ availbility

businesses · adult content → tagging

(P) Or · awareness pgs / splash screen
Or opt-in

triple xxx domain
- require
- available
- expensive

3. tagging

Volentary - industry pratice
or requie tagging

better awaress in educators
└ cyberbullying
better tools

Social medium services that allow it to pervasive

No granularity in age

Should minors be able to communicate online

Me

1. Tagging
2. Avability of Tools
3. Awareness

(I totally ignored cyberbullying)
(Grp argued too much on specifics
All very techy - kids)

Other groups

Don't preempt

Sex register ip log

Education in risks
filtering not trust usebl
Same w/ age verification
better awareness/research

(Im about at this class
know facts + syllabus
* Read it better)

(21)

More like physical world bullying

Creature awareness of how your actions affect people

Anonimity

- mac address tracking actt
- so 1 FB acct per device

Our gap

Educate educator about current social media systems

Self empowerment resources

Parents

(no one ever mentions empower kids!)

(missed last one)

Parental edu

Gov grants to develop SW

Outreach

(15) (22)

Pdf, Have to include mechanism

If educate kids → how reach them?

---

teacher training
recognize signs

---

education : digital citizenship, media literacy

survey
multi-tem, pronged agency Good

---

launch plan
try to actually make a difference

---

next time : advocacy mode

Why

Committee ~~meetings~~ members : be adversarial

Reprint assignment 9/16

Agenda 2013 Activity - in class

Goal: Develop recommendations for the 2013 Administration on the topic of online child protection and cyberbullying. both - seem somewhat different

Group Process: Groups of 6 students work together. Each group includes equal number of 'A' and 'B' students so that each group will have students who have read each of the two policy papers.

Deliverable: Two page briefing memo to the Director of the White House Domestic Policy Council: 1 page

1. problem ~~statement in~~ one paragraph
2. top three policy initiatives the Administration could undertake to address the problem
3. constituency analysis: who will support and who will oppose
4. launch event plan: how should this initiative be announced to the public

} 2 for each

Groups will develop material in class and have until Sunday 16 September to submit a final group paper. The paper may not exceed 2 pages.

Draft 9/16

Intro (theplaz) ; problem statement

Educating Educators (pquimby)

Responding to bullying on the playground has traditionally been a responsibility of teachers. With the advent of the internet, bullying now occurs in different and more technically sophisticated ways. It is incredibly important that educators remain aware of the current risks facing today's youth as increased online interaction with peers, mass distribution of youth-authored content, and limited-visibility communication becomes more common.

could move up

We recommend the White House pursue a campaign encouraging K-12 school districts to include training on cyberbullying in professional development activities. It is critical that existing support systems for students in schools and mandatory reporters are aware of the ways that more traditional harmful behavior can extend into cyberactivity. Training educators to recognize and respond to online activities affecting their student's ability to perform in schools will help further the goal of creating a healthy place of learning for our youth.

; well not really when I did it – crappy curriculum

Learning how to use computers effectively and safely is already a part of many K-12 education programs. We strongly urge the White House to advocate for increased funding for the development of classroom curricula that include cybersafety and cyberbullying awareness programs. It is important that students learn how to deal with situations they will encounter outside the safety of school-endorsed activities.

; grant program

These guys can write well

Self-empowerment (dlaw)

As the Internet becomes increasingly ubiquitous, any effort to ensure the safety of minors must rely on user empowerment methods: any filtering technique that did not depend on user buy-in would interfere with the technological underpinnings that give the Internet its unique openness. When deciding *Reno v. ACLU*, the Supreme Court cited the non-existence of effective and non-intrusive filtering measures as one of the motivating factors in its decision.

rewrite

The report of the Online Safety and Technology Working Group states a similar conclusion: "There is no quick fix or 'silver bullet' solution to child safety concerns, especially given the rapid pace of change in the digital world. A diverse array of protective tools are currently available today to families, caretakers, and schools to help encourage better online content and communications." The report emphasizes the need for a layered approach consisting of educational strategies, parental involvement, and technological measures.

(use reason)

Combine

We recommend specifically that lessons on Internet safety be provided via public schools to students and parents alike, since awareness of Internet dangers is a prerequisite of ameliorating them. These lessons should include a summary of dangers on the Internet, and a summary of the effective technological measures available to parents to monitor or limit the Internet browsing of their children.

Same as before

Requirements on adult-content-providers (jhurwitz)

such

The government cannot require adult content providers to limit access to their sites because case law (such as *Ashcroft v. ACLU*) has shown that such regulations typically cannot pass the strict scrutiny required of content-based speech restrictions. We propose the opposite: rather than penalizing online providers who do not limit access to their sites, we suggest monetarily rewarding websites which actively work to keep minors out.

well, existing movements are not tuned enough

wait what? blocking is better

require filtering

Specifically, we advocate adopting the "tag and flag" approach suggested by the Online Safety and Technology Work Group's report titled "Youth Safety on a Living Internet." The working group observed that it's difficult for filtering software based on whitelists or blacklists to handle rapidly-changing content. One solution posed was to "crowdsource" the maintenance of these lists to community members.

for providers?

We propose that the Federal Communications Commission establish an independent office to oversee crowdsourced tagging initiatives. In particular, this office should establish a trusted, nationwide whitelist and blacklist. It can then provide funding to adult content providers who voluntarily add their own websites to the black list, in addition to providing small monetary compensation to crowdsourced volunteers who add and/or update entries in either list.

gov

providing $ in prob not a good plan

This solution does not restrict free speech in any way because it is still up to the individual Internet user to choose to use filtering software based on these white and black lists. Such a self-empowerment system also has the advantage of letting parents set standards for their own children, rather than enforcing a nationwide set of standards for all minors.

non gov is best

Additionally, notwithstanding the financial incentive, we believe that it is in the best interest of adult content providers to cooperate with the tagging process even though they are not required to do so. Adult content providers may create adult search engines that allow responsible adults to browse for new content on the blacklist. Thus, by working with the tagging efforts, adult websites can help users who want to find their content do so more easily. The end goal is simply to help the users who do not wish to stumble upon adult content on the Internet.

Launch plan and constituency analysis (bbaren)

Could receive tagging

We believe most Americans will prove receptive – or, in the very least, indifferent – to these policy initiatives. We expect a highly positive reception from the adult entertainment industry, as it increases the legitimacy of its online presence and should help shield it from some common and more persistent political attacks. Furthermore, we expect a positive response from software manufacturers – particularly those who stand to financially benefit from increased parental control.

has this died – esp w/ mobile

However, pushback will certainly occur. The various teachers unions and school districts will react unfavorably to integrating cyberbullying into their professional development programs, seeing the initiative as yet another unfunded mandate from the federal level. We also expect the national blacklist initiative to be grossly misunderstood; if not presented with utmost care, the initiative may bring heavy criticism from large swaths of the population, led by the electronic libertarian sector. Should the President announce these initiatives, he must also constantly remind Americans that these initiatives represent steps toward greater parental – not governmental – control.

that's why non-profit

While these issues are important, we do not recommend the President spend valuable political capital to make them top-tier issues – particularly given this year is an election year. Rather, we recommend the President's office introduce the initiatives through the standard news media (e.g., though a White House press conference) and by overhauling OnGuardOnline.gov to give cyberbullying and parental controls a more prominent presence. We further recommend that the President discuss the initiatives during his interactions with Congress.

mention earlier is pretty hidden

Editing

9/16

Back to my old 3
- Awareness
- Tagging
- Availability of Tools

Still mix of ~~p~~ bullying + porn

- gcc
- Silly assignment
- mix together

Or

③ Cyberbullying; Awareness

① Porn; Tools + tagging

② Awareness / Self empowerment

So separate it as 2 diff problems

Combine ~~of~~ 2 adult sections

Radically rewriting

(2)

Could wrap up ~~Constitutional~~ Constituent + launch plan

? Mine missing the elegance of their section?

---

like the broadcast flag

Empower the kids!

Cut a section

We didn't care abt length last time

(4 pgs!

Memo

To: White House Domestic Policy Council
From: Michael Plasmeier, Jacob Hurwitz, Paul Quimby, Ben Barenblat, David Lawrence
Subject: Agenda 2013 Recommendations

The Internet has revolutionized communications. The Internet is one best mediums for freedom of speech ever invented. It has made vast amounts of material available all to listeners over the world. However, the openness of the Internet makes it relatively easy for children to access content which is oriented towards adults. It has also given children a more effective platform for children to bully each other.

In order to address the problem of children having access to adult materials, we propose a new type of filtering software based on 21st century technology. We propose establishing a system which requires adult content providers to "tag" their content as adult content. In addition, we propose the Government fund the creation of a list of adult websites who do not comply with the tagging requirement. We then proposing having the government issue an RFP to fund the creation of a browser add-on which would block tagged and listed content, should a user choose to install it.

To address cyberbullying we suggest additional education aimed at educators and parents about cyberbullying: what is it, how to notice signs, and how to address it.

Adult Content: Tagging

Existing proposals for providers of adult content to prevent access by children have run into problems. Many potential solutions have been discarded either because they were ineffective, violated the user's privacy or both.

We advocate adopting the "tag and flag" approach suggested by the Online Safety and Technology Work Group's report titled "Youth Safety on a Living Internet." We propose requiring providers of adult-content to "tag" their content as adult content. The government should set up a technical working group to establish specific technical requirements, but one early suggestion is to add a "X-Adult-Content: Pornography" line to the HTTP header of each page of adult content.

Congress should pass a law enacting penalties on providers of adult content who do not properly tag their content. The requirement that adult providers tag their material as such has never been tested in Court. However, the courts have found that Congress has the power to set laws that guide freedom of speech - for example requiring permits before protests, setting noise limits, and enacting zoning requirements limiting commercial speech.

We believe this is the least-restrictive way for the Government to protect children from adult content. This tag would be invisible to most users, unless they are using special software programmed to look for the tag. Adding a HTTP header is not technically difficult or expensive. Most existing server software allows the addition of a tag with a one line change in the server's configuration file. There should be a safe-harbor an exemption for content providers who are unaware of the nature of the material uploaded to their platform.

Although international providers of adult materials could still tag their materials, they would not be required to do so. Instead, the Government should issue an RFP to an organization to maintain a list of un-tagged adult material. Any person may submit a URL to the list maintainer for consideration of inclusion onto the list. An employee of the organization would then review the website for the presence of adult content and the lack of literary, artistic, political, or scientific value for minors. Any person or browser could query the list for the presence of a URL or download the entire list. The organization would be required to set up an appeal process where website owners can get their sites removed from the list if they no longer contain adult content.

Adult Content: Filtering

The Government would encourage browser and mobile application manufactures to allow a user to block all content either flagged or on a list. More immediately, the Government would award a grant to a US-based organization to produce add-ons for common Internet browsers that would block flagged and listed content. The add-ons would be freely available and open-source. Other persons or organizations would also be free to set up lists of their own.

Looking for the flag or checking websites against the list is totally optional. When deciding *Reno v. ACLU*, the Supreme Court cited the potential development of effective and non-intrusive filtering measures as one of the motivating factors in its decision. In *Ashcroft v. American Civil Liberties Union,* the Court again found that filters were a less restrictive means of blocking material. The Court also identified some problems with filters, namely inexactness and cost. This proposal addresses the problems by funding the development of a human-curated list of sites. By having the government fund the development of a browser-add on, the Government would address the problem of cost. Having adult providers tag their content as such would the least restrictive way for the government to achieve its objective.

This plan should be popular with both parents who want their kids protected, parents who want more control, as well as the adult-content industry. Those who want to block content from children can enable free filters, those who want to access to the material can leave the filters off. The adult industry can place the accidental access question behind them by making a quick change to their server configuration. Existing filtering software manufactures would still have a place in the market by offering additional features such as keyword blocking or skin tone analysis. There is a risk that the list may be misunderstood. However, devices should continue being able to access that content. Content will only be blocked if a user or the machine owner takes an affirmative step to do so.

Cyberbullying

Responding to bullying on the playground has traditionally been a responsibility of teachers. With the advent of the internet, bullying now occurs in different and more technically sophisticated ways. It is incredibly important that educators remain aware of the current risks facing today's youth as increased online interaction with peers, mass distribution of youth-authored content, and limited-visibility communication becomes more common.

We recommend that the Department of Education produce a curriculum for K-12 school districts to include training on cyberbullying in professional development activities. It is critical that existing support systems for students in schools and mandatory reporters are aware of the ways that more traditional harmful behavior can extend into cyberactivity. Educators should understand what cyberbullying is and the methods children have used in the past. Educators

should know how to look for the signs of cyberbullying and how those may differ from traditional bullying. Educators should also know how the tools available to them to investigate and stop cyberbulling. Educators should be able to teach children how to stand up to and report cyberbulling.

Education should not stop with teachers. Parents should also be aware of the signs of cyberbullying and how to talk with their children about it. The Department of Education should collaborate with OnGuardOnline.gov to improve the depth of the materials available on the site.

Memo

Final

To: White House Domestic Policy Council
From: Michael Plasmeier, Jacob Hurwitz, Paul Quimby, Ben Barenblat, David Lawrence
Subject: Agenda 2013 Recommendations

The Internet has revolutionized communications. The Internet is one best mediums for freedom of speech ever invented. It has made vast amounts of material available all to listeners over the world. However, the openness of the Internet makes it relatively easy for children to access content which is oriented towards adults. It has also given children a more effective platform for children to bully each other.

In order to address the problem of children having access to adult materials, we propose a new type of filtering software based on 21st century technology. We propose establishing a system which requires adult content providers to "tag" their content as adult content. In addition, we propose the Government fund the creation of a list of adult websites who do not comply with the tagging requirement. We then proposing having the government issue an RFP to fund the creation of a browser add-on which would block tagged and listed content, should a user choose to install it.

To address cyberbullying we suggest additional education aimed at educators and parents about cyberbullying: what is it, how to notice signs, and how to address it.

Adult Content: Tagging

Existing proposals for providers of adult content to prevent access by children have run into problems. Many potential solutions have been discarded either because they were ineffective, violated the user's privacy or both.

We advocate adopting the "tag and flag" approach suggested by the Online Safety and Technology Work Group's report titled "Youth Safety on a Living Internet." We propose requiring providers of adult-content to "tag" their content as adult content. The government should set up a technical working group to establish specific technical requirements, but one early suggestion is to add a "X-Adult-Content: Pornography" line to the HTTP header of each page of adult content.

Congress should pass a law enacting penalties on providers of adult content who do not properly tag their content. The requirement that adult providers tag their material as such has never been tested in Court. However, the courts have found that Congress has the power to set laws that guide freedom of speech - for example requiring permits before protests, setting noise limits, and enacting zoning requirements limiting commercial speech.

We believe this is the least-restrictive way for the Government to protect children from adult content. This tag would be invisible to most users, unless they are using special software programmed to look for the tag. Adding a HTTP header is not technically difficult or expensive. Most existing server software allows the addition of a tag with a one line change in the server's configuration file. There should be a safe-harbor an exemption for content providers who are unaware of the nature of the material uploaded to their platform.

Although international providers of adult materials could still tag their materials, they would not be required to do so. Instead, the Government should issue an RFP to an organization to maintain a list of un-tagged adult material. Any person may submit a URL to the list maintainer for consideration of inclusion onto the list. An employee of the organization would then review the website for the presence of adult content and the lack of literary, artistic, political, or scientific value for minors. Any person or browser could query the list for the presence

of a URL or download the entire list. The organization would be required to set up an appeal process where website owners can get their sites removed from the list if they no longer contain adult content.

Adult Content: Filtering

The Government would encourage browser and mobile application manufactures to allow a user to block all content either flagged or on a list. More immediately, the Government would award a grant to a US-based organization to produce add-ons for common Internet browsers that would block flagged and listed content. The add-ons would be freely available and open-source. Other persons or organizations would also be free to set up lists of their own.

Looking for the flag or checking websites against the list is totally optional. When deciding *Reno v. ACLU*, the Supreme Court cited the potential development of effective and non-intrusive filtering measures as one of the motivating factors in its decision. In *Ashcroft v. American Civil Liberties Union,* the Court again found that filters were a less restrictive means of blocking material. The Court also identified some problems with filters, namely inexactness and cost. This proposal addresses the problems by funding the development of a human-curated list of sites. By having the government fund the development of a browser-add on, the Government would address the problem of cost. Having adult providers tag their content as such would the least restrictive way for the government to achieve its objective.

This plan should be popular with both parents who want their kids protected, parents who want more control, as well as the adult-content industry. Those who want to block content from children can enable free filters, those who want to access to the material can leave the filters off. The adult industry can place the accidental access question behind them by making a quick change to their server configuration. Existing filtering software manufactures would still have a place in the market by offering additional features such as keyword blocking or skin tone analysis. There is a risk that the list may be misunderstood. However, devices should continue being able to access that content. Content will only be blocked if a user or the machine owner takes an affirmative step to do so.

Cyberbullying

Responding to bullying on the playground has traditionally been a responsibility of teachers. With the advent of the internet, bullying now occurs in different and more technically sophisticated ways. It is incredibly important that educators remain aware of the current risks facing today's youth as increased online interaction with peers, mass distribution of youth-authored content, and limited-visibility communication becomes more common.

We recommend that the Department of Education produce a curriculum for K-12 school districts to include training on cyberbullying in professional development activities. It is critical that existing support systems for students in schools and mandatory reporters are aware of the ways that more traditional harmful behavior can extend into cyberactivity. Educators should understand what cyberbullying is and the methods children have used in the past. Educators should know how to look for the signs of cyberbullying and how those may differ from traditional bullying. Educators should also know how the tools available to them to investigate and stop cyberbulling. Educators should be able to teach children how to stand up to and report cyberbulling.

Education should not stop with teachers. Parents should also be aware of the signs of cyberbullying and how to talk with their children about it. The Department of Education should collaborate with OnGuardOnline.gov to improve the depth of the materials available on the site.

In order to launch the initiative and draw attention to the new curriculum and website section, the President could hold a press conference at a local elementary school.