The Internet Safety Technical Task Force
Second Quarterly Report to the Attorneys General
June 30, 2008

I. Introduction.

The Internet Safety Technical Task Force was created in February, 2008, in accordance with the Joint Statement on Key Principles of Social Networking Safety announced by the Attorneys General Multi-State Working Group on Social Networking and MySpace in January, 2008. This report is the second of four quarterly reports that the Task Force will submit to the Attorneys General, in addition to the Final Report due on December 31, 2008.

II. Task Force Activities.

Since the last Quarterly Report to the Attorneys General, Laura DeBonis joined the Task Force as Technical Advisory Board Chair. Jessica Tatlock became the Task Force Coordinator. Short biographies of both are attached as Exhibit 1.

Also since the last Quarterly Report, the Task Force has held two full membership meetings. The first, on April 30, 2008, included presentations by members of the Research Advisory Board on the topic of harmful contact experienced by children on the Internet. In addition, the members agreed upon refinements to the scope of the Task Force charter and to the questions the Task Force will address. A revised project plan reflecting these refinements is attached as Exhibit 2.

At the second meeting, on June 20, 2008, members of the Research Advisory Board presented research on children's access and creation of harmful Internet content, an Assistant U.S. Attorney discussed the law enforcement perspective on Internet safety concerns, and six Task Force members proposed technology to improve child safety on the Internet. Minutes of both meetings are attached as Exhibits 3 and 4.

The Task Force has published an Intellectual Property Policy that is designed to protect the intellectual property rights of Task Force members and non-member contributors. The policy is attached as Exhibit 5.

The next Task Force meeting is planned for September 23-24, 2008. The first day will be open to a public audience and to presentations by non-Task Force members. The second day will be the third full membership meeting of the Task Force.

III. Research Advisory Board Activities.

In addition to presenting at the April 30 and June 20 meetings, the Research Advisory Board (RAB) is preparing a literature review of scholarly research on Internet child safety issues that concern the Task Force. A draft of the literature review will be

distributed before the September 23-24 Task Force meeting. The RAB has solicited input from the Task Force members about what topics to review.

IV. Technical Advisory Board Activities.

The members of the Technical Advisory Board (TAB) were selected from a group of candidates recommended by the Task Force, by the Berkman Center, and by technical authorities elsewhere. The goal was to assemble leading experts in technology relevant to protecting the safety of children on the Internet, while avoiding conflicts of interest related to the specific technical approaches under consideration. The TAB roster is attached as Exhibit 6.

The Technical Advisory Board published its call for technology submissions on June 23, 2008. Submissions are due on July 21, 2008 and must follow the template provided on the Task Force website. The template and submission guidelines are attached as Exhibits 7 and 8. The TAB will assess the submissions and report to the Task Force on a typology of the submitted technologies and a corresponding typology of the problems that the submissions are intended to solve.

V. Exhibits.

1. Task Force Leader Biographies
2. Internet Safety Technical Task Force Project Plan, revised June 26, 2008.
3. Minutes of Internet Safety Technical Task Force meeting on April 30, 2008.
4. Minutes of Internet Safety Technical Task Force meeting on June 20, 2008.
5. Intellectual Property Policy
6. Technical Advisory Board Membership
7. Technical Advisory Board Technology Submission Template
8. Technical Advisory Board Technology Submission Guidelines

EXHIBIT 1

Task Force Leader Biographies

Laura DeBonis, Technical Advisory Board Chair. Laura recently left Google where she worked for 6 years on a variety of products and projects. Most recently, she was the Director for Library Partnerships for Google Book Search; she also worked on the launch teams for AdSense Online and Froogle as well as 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, Laura 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.

Jessica Tatlock, Task Force Coordinator. Jess Tatlock joined the Berkman Center in Spring, 2008 as the Coordinator of the Internet Safety Technical Task Force. She holds a Master's in Education and has worked extensively in Boston's youth development and education fields.

Internet Safety Technical Task Force Project Plan
June 27, 2008

I. Background.

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

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

II. Scope.

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

1. Are there technologies that can limit harmful contact between children and other people?

2. Are there technologies that can limit the ability of children to access and produce inappropriate and/or illegal content online?

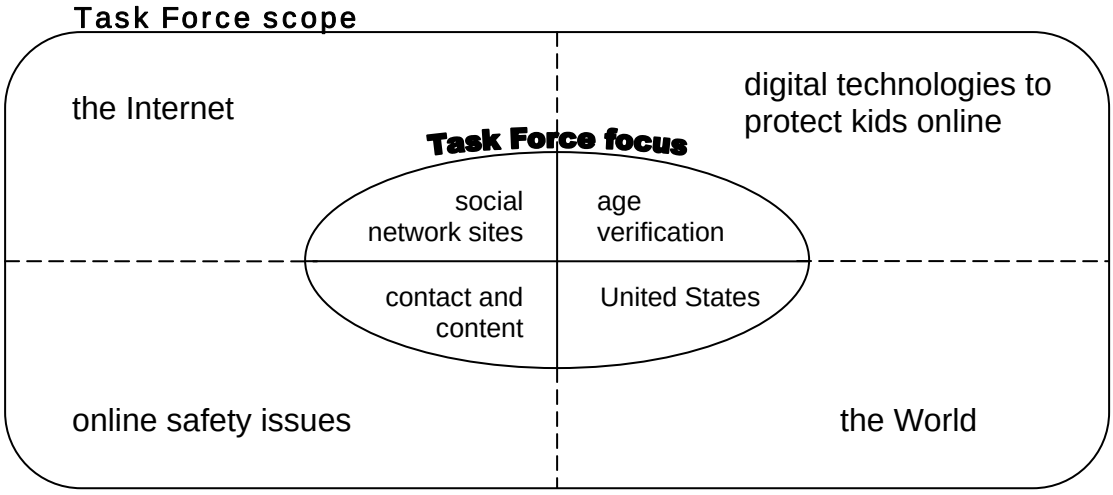
3. Are there technologies that can be used to empower parents to have more control over and information about the services their children use online?

Within each of these broad topic areas, the Task Force will seek to determine the most pressing aspects of the problem and, in turn, which technologies are most likely to help companies, parents, children, and others in addressing those aspects. The inquiry will address all minors (i.e., people under the age of 18), but the Task Force will seek where possible to tailor its recommendations to more refined subsets in age.

The Task Force is chartered specifically to assess age verification technology as a means to reduce the harmful contact and content experienced by children using social network sites in the United States. Popular media have highlighted privacy and safety concerns that arise when children use social network sites[1], but the nature of the danger

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

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



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

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

III. Structure.

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

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

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

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

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

IV. Systems.

A. Reports.

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

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

B. Meetings.

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

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

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

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

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

C. Website and Online Workspace.

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

V. Communications.

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

VI. Intellectual Property.

The Task Force has developed and posted an Intellectual Property 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.

EXHIBIT 3

Berkman Center Internet Safety Technical Task Force
First Full Meeting

Washington D.C.
April 30, 2008

Minutes

Introduction

The meeting opened with brief remarks by Chairman John Palfrey.

Presentation by the Research Advisory Board

Presentations by the Research Advisory Board are not intended to conclusively evaluate the effectiveness of technological or other means to reduce the risks faced by children on the Internet. Nor are they intended to definitively guide efforts to reduce those risks. Instead, the RAB presentations are meant simply to outline the scope of the harmful content and contact experienced by children on the Internet and place those harms in a societal context based upon ongoing research. Task Force members are therefore cautioned not to draw unwarranted conclusions from the RAB presentations.

The meeting began with a presentation by Amanda Lenhart, Senior Research Specialist, Pew Internet & American Life Project, entitled "Teens, Online Stranger Contact and Cyberbullying: What the Research Tells Us." She was followed by a presentation by Michele Ybarra, President and Research Director, Internet Solutions for Kids, who presented "Social Networking Sites, Unwanted Sexual Solicitation, Internet Harassment and Cyberbullying." Next, Janis Wolak, Assistant Research Professor, Crimes Against Children Research Center, University of New Hampshire, presented "Youth Enforcement Surveys by the Crimes Against Children Research Center." Finally, Task Force co-director danah boyd spoke briefly about some of her findings. During each of these presentations, members of the Task Force asked brief, clarifying questions, while further discussion and comment was saved until after the presentations were completed. Copies of the presentation slides can be found on the Task Force Website. In addition, this session was recorded.

Question and Answer with the Research Advisory Board

After a break for lunch, Task Force members were given the opportunity to ask questions of the researcher-presenters.

The first question asked what the research implies about what kinds of education programs should be developed to address these issues. The researchers answered that the issue is not so much whether kids are hearing the message, but whether they respond to it. If you can view media coverage of this issue as an education program, teens are definitely getting the message. Formal education programs might be helpful in terms of

clarification, however, because while kids know about the myth of the 40-year-old lurking in the corner they are not as aware of other risks.

Members also asked about the amount of deception that researchers found online regarding the age of people inappropriately contacting young people on the Internet, and whether this seems to point to less of a need for age verification. Researchers agreed that there was not a lot of evidence to support the deception hypothesis, and that the problem of statutory rape was not going to be solved by age verification.

Researchers were asked, if they had to focus on the top things to do, whether from a technical or education perspective, what they would recommend. The first thing suggested was making inappropriate content, conduct and contact easier to report and creating suggestions for kids to intervene and support safety measures. Education was also suggested, particularly in the areas of statutory rape and inappropriate user-generated content. Another suggestion was to pair up mental health professionals and social network sites and have mental health professionals monitor the sites, reaching out to at-risk kids. Finally, it was suggested that more peer education and peer contacts should be instituted as a more accessible way for kids to talk about issues of safety.

The next question was about formulating intervention strategies and who should be responsible for this? The answer was that the model was that this should be done not through schools, but through partnership of mental health organizations and professionals with social network sites.

Next, members asked about how the process of grooming was taken into account when evaluating the threat of sexual solicitation online. The answer was that during the course of research young people were asked what happened to them, and for the most part the responses did not amount to grooming, which is a process more associated with younger children (because it involves reducing inhibitions to sexuality over time).

The next question was about the use of child pornography as something kids engage in as conduct and something that might be used in contact with them. Researchers said that in their research they have found that the percentage of young people who report looking at pornography is the same online as that who report looking at it offline. Across the board kids do not see creation of images of themselves as child pornography, and they frequently produce it for men who are a little bit older than themselves for the purpose of attracting their attention. This is an issue where education is really important.

Next it was asked whether pre-social network sites like Club Penguin were experiencing the same problems with bullying or sexual solicitation, and the answer was no, less than 10% of those who are solicited or harassed are in these virtual worlds.

It was remarked that the realities of the risks presented by the researchers are not the same as those portrayed in the media and concerned about by the attorneys general. Researchers responded that this is a much more nuanced and complicated issue than

typically portrayed in the media, and that the kids that really need to be reached are the same kids who are already at risk offline.

Next, it was asked why, since it seems plausible that abductors would use the Internet to reach out to kids, why this was not happening more. The answer was that most sex offenders who offend against children and adolescents are not strangers, and that the stranger abductions you read about are really very rare. People who commit those crimes have certain characteristics that the Internet probably is not that favorable to, including the use of authority over younger kids (which does not translate well on the Internet) and the impulsiveness that tends to accompany most stranger abductions (most teens will not actually reveal a lot of information about themselves and so it takes a lot of patience to finally strike up a relationship that leads to an offline relationship).

Finally, it was asked whether anyone has done a larger work using a social network site or something similar to ask kids anonymously whether they have encountered someone offline and been assaulted against their consent. The response was that no study like that has been done to their knowledge, but that the numbers in their studies match up with what is seen elsewhere.

Refinement of Scope and Questions to be Addressed

After the researchers left, the Task Force turned to a discussion of how to refine the scope of its inquiry taking the research into account. First, a reminder was issued that the Task Force is guided by the background of the joint-statement between MySpace and the attorneys general, and the reality that the issues being dealt with are complex and broad-based. Suggested areas of discussion included how to narrow the discussion of content and whether or not Cyberbullying should be included within the scope of the Task Force's inquiry.

The discussion began with the language as expressed in the working document: "preventing harmful contact with adults." Participants initially expressed approval with this language as a broad definition of scope, but the suggestion was made that the Task Force should decide what types of specific contact it was worried about and whether it would further divide its inquiry by age group (ex: one set of recommendations for children 12 and under, another for 13 and over). It was agreed that the different age groups will be relevant regardless of whether the scope is formally limited by age. The suggestion was also made that issues of contact and conduct should be either separated, or that, instead of addressing content separately it should be subsumed within discussions about contact and conduct.

The discussion next turned to the issue of child pornography. Some suggested that issue of child pornography generally was beyond the scope of this group; but that it should consider including the use of child pornography in contact with or the conduct of minors as something to be aware of as the inquiry proceeds.

Questions were asked about the position of attorneys general and what they intended the Task Force's focus to be. It was suggested that the Task Force look at what is happening when there are no "walls" separating adults and children, and the fact that much of the contact that occurs in these situations is "wanted" by teens that are compliant. In response, it was reminded that the charge is to look at technological safety for kids, and that this can be much broader than just age verification and social network sites, and to recognize that the Task Force is dealing with international issues but that the its inquiry will have a domestic scope.

It was next decided that the most productive way to discuss scope would be to go through the five questions discussed at the last meeting. In doing so, it was suggested that the questions be reworded to ask, what are the technologies that will assist in limiting, rather than stopping, the harm identified. The questions were then discussed in turn.

1. *Is there a technology that can limit harmful contact between adults and children?*

Everyone agreed that as a general principle this question should be included in the scope. Concerns were raised about whether the unwanted contact should be defined in terms of the desires of the parents (what parents don't want) or the children (what kids don't want) or both, because these perspectives can vary widely. It was suggested in response to this that the AGs were likely most concerned with empowering parents and allowing them to make the decision as to what is and is not harmful for their child.

Additional concerns were raised about limiting the scope of this question to harmful contact between adults and children, or if it should be expanded to include child to child contact. Part of this concern was driven by the feasibility of technology being able to differentiate children and adults online in a reliable way. Also driving these concerns were the results of the research presented earlier in the day which suggested that the most frequent contact is peer-to-peer rather than adult-child.

2. *Is there a technological solution to limiting children from accessing inappropriate content on websites?*

Concern for this question was that if the Task Force took on too many projects during its limited tenure its inquiry would fail. Suggestions were made that market forces are already placing tremendous incentives in front of the production of tools that parents can use to limit their children's access to inappropriate content, and that the market may be better suited than the Task Force at tackling this particular problem. It was also suggested that, to the degree that market forces are successful, there is a risk that regulation can get in the way.

An alternative concern was raised that the Task Force should focus less on child access to inappropriate content than on child production of inappropriate content. Some children

are producing inappropriate content on their profiles in social network sites or on their cell phones.

Others suggested that, rather than taking on child pornography or other inappropriate content on the Internet, the Task Force should start with the foundation that has been laid by older studies and issue and update or addendum to these studies. One way of updating these previous studies would be the inclusion of methods to address user-generated content, because this is a relatively recent phenomenon, and that the focus be on Web 2.0 rather than social network sites alone.

3. *Is there a technological solution to limiting the availability of illegal content?*

There was a great deal of discussion regarding whether or not illegal content should be included in the scope of the inquiry. It was suggested that if this content were address, it should include child pornography and gambling, but not copyrighted material. It was also reiterated that perhaps user-generated content should be within the scope of the inquiry but commercial or other child pornography should and is being dealt with elsewhere. Another suggestion was made that if the Task Force is going to branch out into all of these different areas, it should consider breaking up into smaller subcommittees in order to work more efficiently.

Also heavily discussed was the meaning of "illegal" content and what should be included in this question. It was argued that copyright should not be included, and this was generally agreed on although no consensus was reached. It was suggested that illegal be more narrowly defined and the touchstone of what is illegal should also be harmful.

Finally, a non-binding straw poll was taken and the majority present agreed that this should not be a separate question, but that it should be folded into question two, which should deal with the production of inappropriate user-generated content.

4. *How do you prevent children from getting onto social network sites without parental consent?*

First, it was suggested that this should be rephrased to ask, is there a technological solution that has the capability to allow parents to block access to social network sites, if they so desire? To this is was pointed out that kids do not typically access these unwanted sites in the home, and that they also know proxies and are very good at getting around filtering software.

Concerns were expressed about focusing on something narrow – such as social network sites – rather than at-risk kids more generally. It was also pointed out that the reality of social networking encompasses much more than just Facebook and MySpace, and that it includes instant messaging, Amazon accounts, and anywhere else you can create a profile and communicate with others.

It was next suggested that the question be reframed again, to say: How can we give parents the ability to shut down a kids profile under certain circumstances? The suggestion was made that if a parent can be confirmed as the parent with legal custody over that child and the child is younger than a certain age, the parent should be able to contact the company and have the child's profile removed. This rephrases the focus from preventing access to empowering parents and giving them more control, in exchange for placing the burden on parents.

In response to this, a final wording of this question was suggested: What tools and technologies can be used to empower parents to have more control and information over the services their children use?

5. *How do you prevent young people from engaging in bullying, harassment, and unwanted solicitation?*

It was suggested that this question should focus on empowering kids to prevent, avoid and self-report cyberbullying. Immediately, however, concerns were raised that this question was already encompassed by the discussion in question one. Additional concerns were raised that bullying and harassment do not fall within the concerns of the Task Force, that this is not what the attorneys general had in mind, and that, given the limited time frame, this question should not be included. Others pointed out that this is the next big issue and the Task Force ought to address it.

A non-binding straw poll was taken, and it was agreed that instead of focusing on cyberbullying as its own question, it should be folded into the first question as peer-to-peer predation and violence.

Ultimately, the Task Force discussed compressing the five original questions in to the following three:

1. *Is there a technology that can limit harmful contact between children and other people?*
2. *Is there a technology that can limit children from accessing or producing inappropriate and/or illegal content online?*
3. *What tools and technologies can be used to empower parents to have more control and information over the services their children use online?*

<u>Logistics</u>

The meeting concluded with a brief discussion of logistics. First, some members of the Task Force have expressed reservations about using email as the primary mode of discussion. The Berkman Center will work on arranging another method of in-between conversations, such as conference calls. Second, some members have expressed concern that they are being approached for business as part of this Task Force, and it is extremely important this not occur. Third, Task Force members were reminded that it is inappropriate for members to represent to the attorneys general what individual members of the group are saying. This is not a gag order, but a formal mechanism of quarterly reports is in place to communicate with the attorneys general.

Finally, because other discussion ran long, an update about the Technical Advisory Board will be sent out via email. Laura DeBonis, formerly of Google**,** will chair the board and help come up with other members. All members of the Task Force are encourage to make membership recommendations, though it should be remembered that these should be limited to people with as little financial encumbrance as possible.

The next meeting will take place on June 20, 2008 in Cambridge, Massachusetts.

EXHIBIT 4

Berkman Center Internet Safety Technical Task Force
Minutes of the Second Full Membership Meeting

Cambridge, Massachusetts
June 20, 2008

Introduction

Task Force Chairman **John Palfrey** opened the meeting with welcoming and administrative remarks

Research Advisory Board Presentations

The Research Advisory Board (RAB) presentations by Michele Ybarra and danah boyd were video recorded and will be made available to the public.

Presentations by the Research Advisory Board are not intended to conclusively evaluate the effectiveness of technological or other means to reduce the risks faced by children on the Internet. Nor are they intended to definitively guide efforts to reduce those risks. Instead, the RAB presentations are meant simply to outline the scope of the harmful content and contact experienced by children on the Internet and place those harms in a societal context based upon ongoing research. Task Force members are therefore cautioned not to draw unwarranted conclusions from the RAB presentations.

Task Force Co-Director **danah boyd** introduced this session. She informed the Task Force that the RAB is preparing a literature survey of non-policy documents on Internet child safety, and solicited input from Task Force members. She also indicated that unlike the April 30 meeting, which focused on harmful contact between adults and children, the RAB presentations of this meeting would address harmful content. There has been relatively little research on the mechanisms and effects of harmful content.

Michele Ybarra, President and Research Director, Internet Solutions for Kids, Inc., presented "Youth Exposure to Pornography and Violent Web Sites." Michele drew from the Growing Up with Media survey and the Youth Internet Safety surveys. She compared intentional to unintentional exposure to X-rated material.

Unintentional Exposure to X-rated Content—The majority of children's exposure to X-rated content on the Internet is unintended, and the likelihood of exposure increases with age. These trends are observed both in the U.S. and the U.K. Unintended exposure does not appear to pique the interest of the kids exposed, based on the observation that only 2% of those who are unintentionally exposed to X-rated content intentionally return to the X-rated site.

Intentional Exposure to X-rated Content—Roughly 20% of children seek out X-rated content on the Internet, making it less popular than other sources of such material. Children who do look for such content on the web are generally 2-3 times more likely to

engage in other negative behavior, such as physical bullying and getting into fights, than children who do not. According to Michele, these children "have a lot going on in their lives."

Violent Content—Only 2% of children intentionally visit hate sites; 4% visit death sites; but 22% visit violent cartoon sites such as stickdeath.com, which is troubling because the combination of violence and humor on such sites has a greater impact on children. The psycho-social profiles of children who seek violent web content reveal that they are subject to the same increased odds of negative offline behavior as those who seek out pornographic content.

Questions and Answers:

1. Does the data distinguish between X-rated content in movies streamed online versus videos on YouTube? Kids think of YouTube as "YouTube," distinct from Internet movies, suggesting that YouTube viewing is excluded from these data.
2. Other research has suggested that affluent children home alone in the suburbs seek out X-rated content at a high rate. Is this finding consistent with Michele's conclusion that children who seek out X-rated content on the Internet are likely to also experience a variety of psycho-social difficulties? A child is no less likely to experience psycho-social troubles because he or she is affluent and lives in the suburbs. Therefore the two results are consistent. danah added that having workaholic parents is a very strong indicator for children getting into harmful content on the Internet.
3. Since the negative behaviors, such as physical bullying and fighting, that are more likely in children who seek X-rated Internet content are anti-social, are these children less likely to be involved in social network sites? This is not known from the available data, but online communities do exist even for individuals who are anti-social offline.

Next, **danah boyd**, Berkman Center Fellow, presented qualitative results on problematic youth-generated content. The vast majority of youth do not participate online in this manner, but there is no available quantitative data on the topic. danah offered to match researchers with companies or institutions who wish to fund further work in this area.

Youth-created pornographic content—Girls are more likely than boys to post sexually suggestive photos of themselves online. Youth-generated pornographic content falls into four categories: 1) sexually suggestive still photos in which the creators "strut their stuff," 2) dance videos that are set to popular music and emulate MTV videos, 3) pornographic or nude photos that would be illegal if produced by an adult, and 4) Paris Hilton-style videos of the creators having sex with other minors. The primary intended audience for this material is heterosexual boys, but in some cases the pictures are meant to get attention from modeling agencies or mark a girl's status among her peers. The images often are intended to be available only among the child's friends, but nevertheless end up circulating widely.

Other youth-created content—In addition to providing pornographic content, youth contribute a variety of harmful content to user-generated websites. Some of this includes: fight videos, "shock" content, self-harm imagery (including pro-ana, pro-mia and self-injury images).

Questions and Answers for both presentations:

1. None of the sample images in danah's presentation show faces. Do the kids generally post images without faces? No, generally the kids who post their images intend for friends to be able to identify them and freely include their faces.
2. Do children tend to grow out of providing inappropriate images of themselves? Michele Ybarra referred to data suggesting that between an initial survey and a follow-up, a third of the children persisted, a third stopped, and a third started posting images of themselves.
3. The presentation focuses on the most extreme online behavior. Aren't cases of 14 year-olds accessing R-rated material equally troubling? The research itself focuses on the most extreme behavior.
4. Do adults use the child-provided content to create child pornography? Unknown: that is outside the scope of this research.
5. How many children go to cutting sites? The only data available is for self-harm sites in general, and not specifically cutting.
6. How are social network sites attempting to deal with self-harm content? Online communication on these topics tends to be thoroughly encoded and therefore very difficult for technologists to identify and filter. danah is currently working on a project to bring together researchers, child psychologists, and technology companies to get a better solution to this issue.

Break

Task Force Chairman **John Palfrey** thanked the Research Advisory Board for pointing out not only what we do know, but also what we do not. He emphasized that the all of the day's remaining presentations would be recorded for Task Force use only and would not be made public.

Law Enforcement Perspective

Task Force Co-Director **Dena Sacco** then introduced **Ms. Dana Gershengorn**, Assistant United States Attorney for the District of Massachusetts. Ms. Gershengorn spoke from a law enforcement perspective about trends in youth online safety and responded to Task Force questions. She focused on child enticement instead of classic child exploitation like sex tourism and presented observations from both proactive and reactive law enforcement activities.

Technical Advisory Board Presentations

Laura DeBonis, Chair of the Technical Advisory Board (TAB), introduced the TAB members present and announced that the TAB would publish its call for technology

submissions on June 23, 2008. Submissions are due on July 21, 2008 and must follow the template provided on the Task Force website. Task Force members presenting technology at today's meeting are required to formally submit a proposal according to the TAB template in order for their technology to be evaluated and included in the Task Force report.

John Clippinger, Berkman Center Fellow, introduced the concept of an identification metasystem for the Internet as a means to overcome its lack of an identity layer.

Mike Jones and Jules Cohen of Microsoft Corporation presented a conceptual use of digital Information Card technology.

Andrew Wharton, Chief Technology Officer and Chief Architect of Sentinel Technology, (together with **John Cardillo** via telephone) presented one existing Sentinel product, the Sentinel Safe database of registered sex offenders, and one proposed product, Sentinel Kid Safe.

John Dancu of IDology, Inc., presented "Examining Identity and Age Verification" and recommended that the Task Force arrange for an overview presentation of authentication technology by a consultant from either the Burton Group or Gartner, Inc.

John Phillips, CEO of Aristotle, discussed proposed approaches to age and identity verification.

David Lee of Symantec presented Norton Family Safety, a planned product currently in private beta testing.

Drew Weaver of America Online presented the evolution of online safety products at AOL.

Wrap-up

John Palfrey made the following points in conclusion.

1. The next Task Force meeting is planned for September 23-24, 2008. The first day will be open to a public audience and to presentations by non-Task Force members. The second day will be the third full membership meeting of the Task Force.
2. Over the course of the next month, the Technical Advisory Board will receive technology submissions. The TAB will report to the Task Force on:
    a) a typology of the submitted technologies;
    b) a corresponding typology of the problems that the submissions are intended to solve; and
    c) an assessment of whether the submissions will be effective.
3. Task Force Scope— The Attorneys General are comfortable with the Task Force scope, namely a focus on age verification technology to reduce contact and content

harmful to children on social network sites in the United States, but flexibility to place this problem in a broader context.
4. The Task Force has submitted one quarterly report to the Attorneys General and will submit the second one shortly after June 30, 2008.
5. Status of Subgroups—No Task Force member has yet opted-in to a subgroup, but the Berkman Center will continue to support the subgroups as required.
6. One Task Force member requested that a social network site operator address the Task Force on the topic of lessons learned—what works and what does not in protecting children.

EXHIBIT 5

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 6

Technical Advisory Board Membership

Members:

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

Affiliate Members:

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

EXHIBIT 7

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.

EXHIBIT 7

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 sub-sections 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 8

Technical Advisory Board Technology Submission Guidelines

Technical Advisory Board

Objective

The objective of the Internet Safety Technical Task Force's Technical Advisory Board (TAB) is to evaluate and assess the range of technologies that may be used to promote children's safety on the Internet.

The Review Process

The TAB will undertake a technical review of the technologies submitted for its consideration and make public the results of this review. The review will attempt to determine whether the technologies works as described and how well protected they are from circumvention. The review will also attempt to determine the infrastructure and the operational requirements for the technologies.

The Role of TAB Members

TAB Members participate fully in both the design and execution of the review process for the technologies submitted for its consideration. Only Members will participate in the actual review process and only they will generate final conclusions and recommendations for the Task Force.

The Role of TAB Observers

TAB Observers will participate in the design of the review process but not the execution of the reviews. Observers typically have useful industry experience and domain expertise, but also potential conflicts of interest. To mitigate any potential for bias, their involvement with the TAB must be limited. So, to be explicit, Observers have already and will continue to assist in the development of the review process (e.g the creation of the Submission Template, the development of a taxonomy, the Evaluation Form) but they will not participate in the actual review process itself. Observers will, however, have access to the technology submissions and can submit a document called an "Observer's Comment" for any technology they choose that will be included in the final documentation of the TAB's work to the Task Force.

Call for Technology Submissions

The TAB is asking to receive submissions from individuals, companies, organizations, etc., with technologies relevant to child safety on the Internet. While this Task Force is focused in large measure on age verification technologies in the context of social network sites, we are not limited to any specific type of application; we are also interested in technologies that address other types of social media (IM, chatrooms, texting, etc.) as well as those that address Internet access more broadly. We will review these

submissions and ask for further information and/or in-person presentations for technologies that have significant promise or about which we have questions.

Some categories of technology we are interested in receiving submissions for include but are not limited to: filtering, blocking, parental controls, labeling, rating, identification, authentication, age verification, imaging, search, and forensics.

Submission of Technologies for Review

To guide this process, we have prepared a Template for submissions. The Template is a formatted Word document that you should download and use to prepare your submission. The Template includes formatting information as well as notes about what you should include. The audience for your submission is technical, consisting primarily of computer scientists; your submission should be written with that audience in mind.

To have your technology included in the Technical Advisory Board's evaluation, **please download the Template below, fill it out, and submit it as a PDF to** tab@cyber.law.harvard.edu**.** This submission will be given to all TAB members for review and it may be made available to the public. We ask that you use the Template for consistency of style and content – please do not submit a press release or PowerPoint deck.

The deadline for submission is July 21, 2008.

Internet Safety Technical Task Force Technology Submission Template

Should we have any questions or follow up about your submission, we will contact you. Should you have any questions for us, please contact Jessica Tatlock at jtatlock@cyber.law.harvard.edu. We apologize in advance that we may not be able to respond to all inquiries.

Legal Disclaimer: *The Berkman Center, the Task Force and Task Force members, and the Technical Advisory Board, including its members and observers 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.*

As described in the submission Template, you must certify along with your abstract or proposal that you have read and agree to the IP Policy, and you must grant the Berkman Center and the Task Force a license to publicly post your submission and use it to carry out the Task Force's work and develop the Task Force's reports.

EXHIBIT 8

Technical Advisory Board, Members

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

Technical Advisory Board, Observers

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