APPENDIX E:

Submissions from Social Network Sites

Internet Technical Safety Taskforce – Request for Input
Bebo and AOL

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

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

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

1. Traditional categories of potential online risk, which include conduct, content, and contact; and

2. Young people becoming perpetrators as well as the victims of harm.

Categories of Potential Online Risk: These categories include:

1. Inappropriate content, which includes exposure through the Internet to pornography, violence, racist content, misinformation and propaganda that can negatively impact young people.

2. Inappropriate contact, which includes contact between adults with a sexual interest in children, or by young people who solicit other young people.

3. Inappropriate conduct, which relates to how young people behave online through social networks. Problems here include:

    a. Bullying or victimization, which includes behaviors such as spreading rumors, excluding peers from one's social group, and withdrawing friendship or acceptance, or

    b. Risk-seeking behaviors, which includes, divulging personal information, posting sexually provocative photographs, lying about real age or arranging to meet face-to-face with people only ever previously met online.

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

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

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

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

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

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

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

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

BEBO

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

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.

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.

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

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

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

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

Company Overview:

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

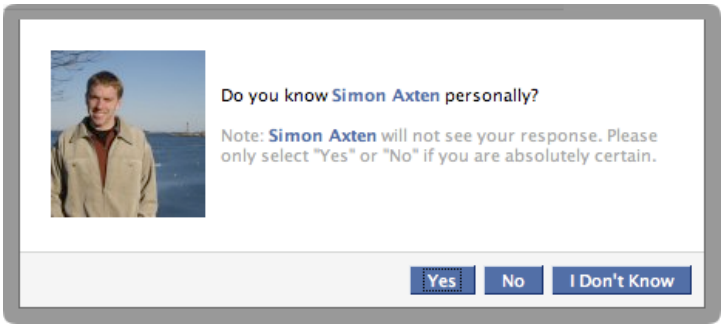
Relevant URLs: www.facebook.com
www.facebook.com/privacy
www.facebook.com/help.php

1. The principal safety issue Facebook works to address is anonymity. While appropriate in some settings, fake names and hidden identities are incongruous with Facebook's goal of allowing people to share and communicate more openly and efficiently. When users are allowed to misrepresent themselves, trust and accountability break down, and people feel less confident in their interactions. Bad actors are emboldened because there is little chance of serious consequence. Most of the systems and processes we have developed are intended to solve this root problem, and we measure the risk that youth face on our site by how well we are doing in this effort.

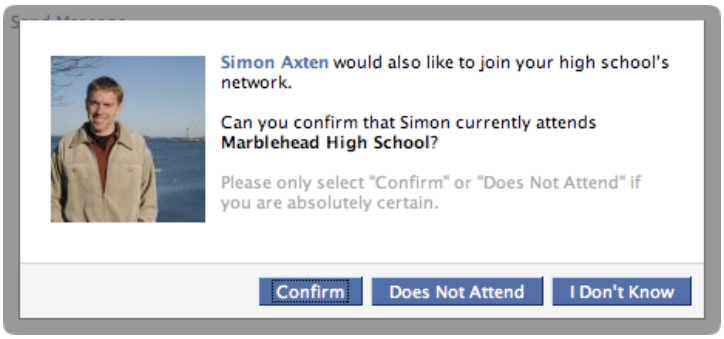
2. Facebook's network-based architecture strives to reflect as closely as possible real world social communities. By default, users' profiles are only available to those who share networks with them or have been confirmed as friends.

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

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

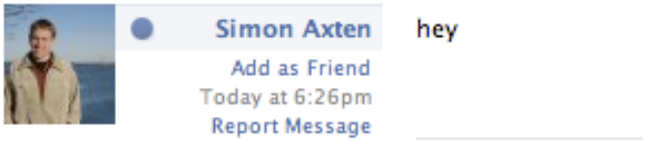


   A high school network affiliation must be established through the process above before a user can gain access to the profiles of others on that network. Users must be 18 or under to join a high school network.



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

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



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

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

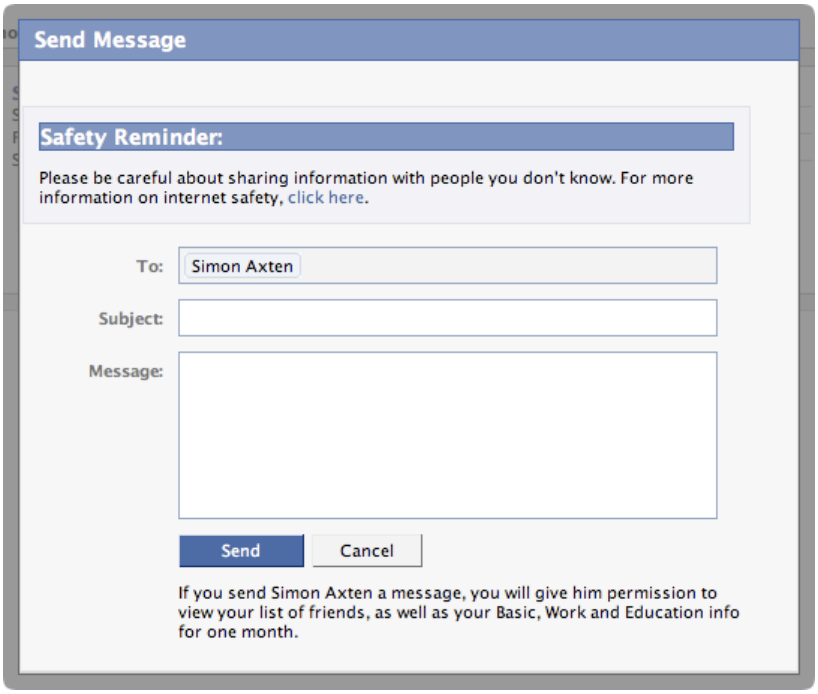
People who try to sign up with a birth date that makes them under 13 are blocked, and a persistent browser cookie is used to prevent further attempts at sign-up.

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

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

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

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



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.

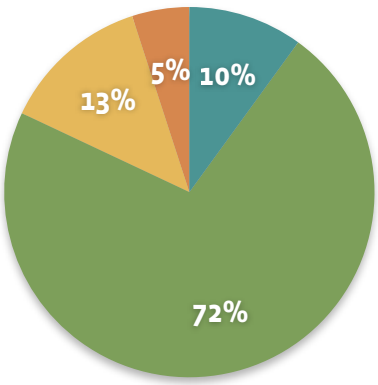
We are deeply committed to our own efforts in this area and believe the controls and processes we have built are leading the industry. At the same time, we recognize that protecting children online is an ongoing battle that requires cooperation among various groups, and we are always open to working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

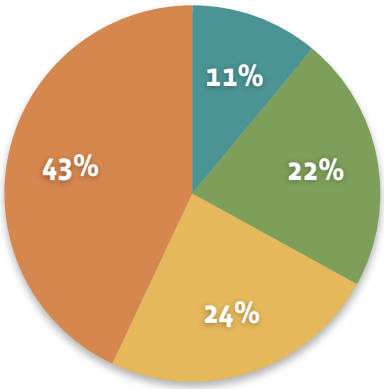
   We have also used our own Polling feature to gauge how minors are using the site, as well as how safe they feel on Facebook relative to other sites and the Internet at large. The results of a few of these polls, which use a sample of 500 users in the US aged 13-17, are below:

Have you ever seen nudity…

…on Facebook?



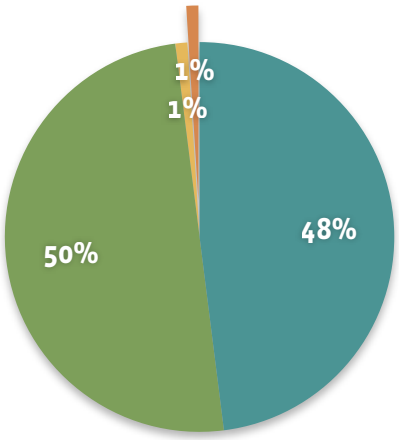
…on a website other than Facebook?



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.

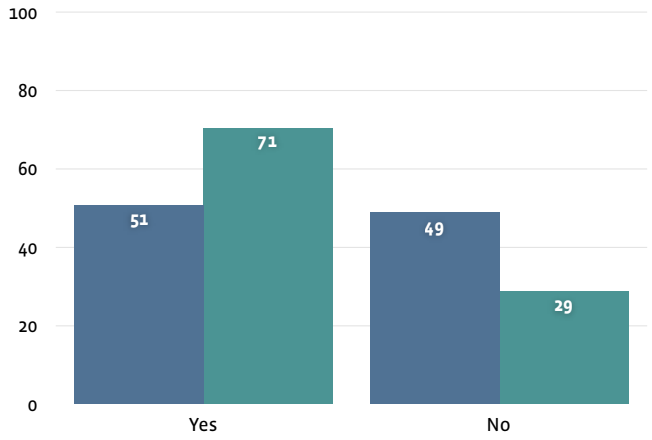
Do you know the people you interact with on Facebook in real life?



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.

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.

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

MySpace Safety, Security and Privacy Overview

MySpace is committed to making our community as safe as possible for all of our members. Safety, security, and privacy are built into every new site feature and we have designed and built features specifically to enhance the security of our online community. This is an ongoing process that we are constantly reviewing and updating under the leadership of our Chief Security Officer, Hemanshu Nigam, who spent 18 years as a career prosecutor and child safety advocate. Nigam is a former Department of Justice Internet crimes prosecutor who held executive-level security positions at Microsoft and the MPAA and who leads a team that works full-time on safety and security-related initiatives across the company. In addition, MySpace has a robust team dedicated to policy enforcement and content review that work to identify potential problems and takes immediate action when safety and/or security issues occur.

We work hard to provide users with access to age appropriate content, to shield younger users from older members of the community, and to partner with law enforcement in these efforts. Some of the most significant steps we have taken in this area include:

Preventing Underage Users

- Our Terms of Use indicate that users must be 13 yrs of age or older to utilize our site
- We employ a search algorithm, utilizing terms commonly used by underage users, to seek and weed out individuals misrepresenting their age
- Additionally, our team actively searches out underage users by hand
- We delete thousands of profiles per week for misrepresenting their age

Protecting Younger Users from Inappropriate Contact

- Users under 18 are automatically assigned a Private Profile upon account creation
- No user can browse for users under 16
- Adults can never add under 16's as a friend unless they know the under 16's last name or email address (adult must know the user in the physical world)
- If users under 16 override their privacy settings, they are still only viewable by other users under 18
- Mature groups cannot be accessed by under 18's

- Users under 18 can block all users over 18 from contacting them or viewing their profile
- 13-15 yr olds are tagged to be un-searchable by age on search engines
- 13-15 yr olds can only receive group invites from the individuals in the friend network
- Users under 18 cannot access age-inappropriate areas such as Romance and Relationship chat, forums and groups, Mature groups and certain Classified categories including dating and casting calls
- Users under 18 cannot browse for age inappropriate categories such as relationship status, smoker, drinker, or income
- Users over 18 are limited in their ability to search in the School section- they can only search for high school students graduating in the current or upcoming year
- The creation and implementation of an adult website database that restricts users from posting mature links on their profile

Protecting Younger Users from Inappropriate Content

- Hosted images and videos are reviewed for compliance with Terms of Use (this includes over 10 million new images and videos uploaded everyday)
- Known inappropriate URLs are blocked from being posted on the site
- IP logs of image uploads are captured
- User accounts deleted for uploading pornographic videos
- Alcohol related ads prohibited from reaching under 21's
- Smoking/Drinking preferences blocked for under 18's/under 21's
- Groups and classifieds are reviewed when inappropriate content is suspected
- Users under 18 are defaulted in a way that requires them to pre-approve all comments made on their profiles

Reporting Inappropriate Content

- Users can report inappropriate content or behavior to MySpace
- Users can report spam email complaints to MySpace
- Users can directly report sexually explicit conduct to NCMEC's CyberTipLine
- Users can easily "Report Abuse" in email, videos, forum posts and classifieds
- Users are easily able to provide reasons when reporting images for Terms of Use violations

Providing Tools for all Members

- All users can set profile to Private
- Users can pre-approve all comments before being posted
- Users can block another user from contacting them
- Users can conceal their 'online now' status
- Users can prevent forwarding of their images to other sites
- Users over 18 can block users under 18 from contacting them or viewing their profile
- All users can allow only those users whom they have proactively added to their Contact List to see when they are on IM and to contact them

- Users can make all their photos, or sections of their photos, Private
- 32,000 school moderators oversee school forums

Providing Education

- All users under 18 receive security warnings before posting content
- All users under 18 must review and scroll through Safety Tips when they sign-on to the site
- Safety Tips link on every page which includes links to parent monitoring and blocking software
- Contact MySpace link on every page
- MySpace Parent Brochure available on Parent Safety Tips page
- School Administrator's Guide to Understanding MySpace and Social Networking Sites distributed to over 55,000 schools.
- Aggressive education campaign through MySpace, News Corp properties, and third-party partners including National Center for Missing & Exploited Children, National PTA, AdCouncil, Seventeen Magazine, National School Board Association & the National Association of Independent Schools.
- Extensive PSA campaigns across News Corp properties

Partnering with Non-profit Organizations

- Partnerships with the Illinois Library Association and the American Library Association to distribute millions of bookmarks on Internet safety in public libraries across the U.S.
- AMBER Alerts: MySpace partners with the National Center for Missing & Exploited Children to distribute localized online AMBER alerts via MySpace so MySpace users can help bring a missing child home
- Education Partnerships with organizations such as ConnectSafely.com, NetFamilyNews.com, WiredSafety.org, I Keep Safe Coalition (iKeepSafe.org), Cyberbullying 411, Enough is Enough and MySpace MyKids
- The donation of Sentential SAFE to NCMEC
- Participate in the UK Government Taskforce on Child Safety on the Internet
- Contributed to the UK Home Office Taskforce's first UK Social Networking Guidance
- Participate in the UK Government's Cyberbullying TaskForce
- Participate in the Australian Government's Consultative Working Group on Cyber-Safety
- Participate in the EU Social Networking Task Force

Partnering with Law Enforcement

- Ongoing support for local, state, and federal law enforcement in investigations and prosecutions
- 24/7 dedicated hotline and email created for use by law enforcement – not just for emergencies
- Ongoing training provided to cyber crime units on how to investigate and prosecute cyber criminals using MySpace

- Law Enforcement Guide and One Sheet created to help law enforcement agencies understand MySpace and investigate cases

Dedicated MySpace Teams

- Customer Care Team: handles sensitive user issues within 72 hours
- Content Assurance Team: ensures integrity of safety systems and flags potential flaws
- Parent Care Team: dedicated parent hotline, email (parentcare@myspace.com) and guidebook
- School Care Team: dedicated educator hotline, email (schoolcare@myspace.com) and guidebook
- Law Enforcement Team: dedicated hotline, email (lawenforcement@myspace.com) and guidebook
- Security Incident Response Team: dedicated security team that works to identify potential problems and takes immediate action when security issues occur

Application Information and Data Collection

- Applications are governed by the same privacy controls that are in place for members
- An application can only get information from the user if the user installs the application and thereby grants the application permission
- MySpace offers a universal setting for not sharing any data, including public information, with any applications

Application Security

- All applications must use our API's, which have security features built in
- All applications go through a robust security review process before going live to our members
- MySpace takes action against applications that violate safety and security requirements

Taking Ongoing Safety/Security Measures to Spot & Solve Safety Challenges

- Email verification required for all new MySpace members
- ParentCare: MySpace developed software, called ParentCare, to help parents easily determine whether their teen has a MySpace profile, learn about safety and to ensure their teen's age is accurate.
- Email Registration Legislation: MySpace supports and has testified in favor of, federal and state legislation that would require registered sex offenders to register all of their email addresses, so that we can block them from accessing our site in the first place.
- Joint Statement on Key Principles of Social Networking Safety: MySpace and Attorneys General in the Multi-State Working Group on Social Networking representing 49 states and the District of Columbia joined forces to unveil a Joint Statement on Key Principles of Social Networking Safety designed for industry-

wide adoption. This common set of Principles relates to online safety tools, technology, education and law enforcement cooperation.

These measures represent just a sampling of the steps MySpace has taken to protect our community's safety and enforce our rules.

APPENDIX B

JOINT STATEMENT ON KEY PRINCIPLES OF SOCIAL NETWORKING SITES SAFETY

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

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

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

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

I. ONLINE SAFETY TOOLS

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

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

- MySpace will organize, with support of the Attorneys General, an industry-wide Internet Safety Technical Task Force ("Task Force") devoted to finding and developing such online safety tools with a focus on finding and developing online identity authentication tools. This Task Force will include Internet businesses, identity authentication experts, non-profit organizations, and technology companies.

  FORMED and ONGOING, LED BY HARVARD LAW SCHOOL'S BERKMAN CENTER FOR INTERNET & SOCIETY

- The Task Force will establish specific and objective criteria that will be utilized to evaluate existing and new technology safety solutions.

- MySpace and other members of the Task Force will provide adequate resources to ensure that all reasonable efforts are made to explore and develop identity authentication technologies.

  DONE

- News Corporation will designate a senior executive to work with the Task Force.

  DONE

- The Task Force will provide the Executive Committee of the Attorneys General Social Networking Working Group ("Executive Committee") with quarterly reports of its efforts and presentation of a formal report by the end of 2008. The Executive Committee will have continuing access to the Task Force and the designated senior executive of News Corporation.

  ONGOING

II. DESIGN AND FUNCTIONALITY CHANGES

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

- MySpace and the Attorneys General share the goal of designing and implementing technologies and features that will make MySpace safer for its users, particularly minors. More specifically, their shared goals include designing and implementing technologies and features that will (1) prevent underage users from accessing the site; (2) protect minors from inappropriate contact; (3) protect minors from inappropriate content; and (4) provide safety tools for all MySpace users.

- The Attorneys General acknowledge that MySpace is seeking to address these goals by (1) implementing the design and functionality initiatives described in Appendix A; and (2) working to implement the design and functionality initiatives described in Appendix B.

- MySpace and the Attorneys General will meet on a regular basis to discuss in good faith design and functionality improvements relevant to protecting minors using the Web site.

  ONGOING (2 written reports submitted regarding the status of implementation of new initiatives, and 1 conference call with Executive Committee members regarding the status of implementation of new initiatives)

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

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

- MySpace will continue to dedicate meaningful resources to convey information to help parents and educators protect children and help younger users enjoy a safer experience on MySpace. These efforts will include MySpace's plan to engage in public service announcements, develop free parental monitoring software, and explore the establishment of a children's email registry.

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/=

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.