facebook

Testimony of Timothy Sparapani
Director, Public Policy
Facebook

April 29, 2010

Before the U.S. Senate Committee on Commerce, Science and Transportation
Subcommittee on Consumer Protection, Product Safety, and Insurance

An Examination of Children's Privacy:
New Technologies and the Children's Online Privacy Protection Act

The Role of Innovation in Creating a Safer Online Environment – the Facebook Experience

Thank you Chairman Pryor, Ranking Member Wicker and Subcommittee Members. My name is Tim Sparapani and I am Director, Public Policy for Facebook. Thank you for inviting me to testify today concerning Facebook's perspective on online child safety. We are pleased to discuss some of our innovations that lead to a safer online environment. We believe these innovations – some of which are obvious to users and others that are not – are a key to providing a positive online experience.

Facebook started in 2004 as a social networking site for college and university students and from inception, Facebook sought to provide a safer environment for all its users than was generally available on the web. Although Facebook is not directed to young children – you must be 13 years of age or older to join Facebook – the Company takes special steps to insure that users under 18 have a safer experience. [1]

Facebook has been involved with many online safety initiatives around the world, such as the US State Attorneys General Internet Technical Task Force, the UK Home Office Task Force on Child Safety, the EU Safer Internet initiative, the Australia Attorney General's Online Safety Working Group and others. Today, I would like to discuss the important ways that Facebook innovation helps promote a safer online environment. We also encourage Congress to encourage, not discourage or prohibit, companies' innovation in policies and technologies to promote child online safety, security and privacy. We believe that our innovations in teen online safety, security and privacy advance the cause of online safety for children.

Summary of Key Points and Request for Congressional Action

We wish to emphasize four points today and enlist Congress' assistance to advance child online safety.

- **Facebook's real name culture and innovative technologies and policies enhance online safety and privacy for teens.**

- **Facebook expends extensive effort on key teen safety issues that further reduce teen risks.**

- **Facebook collaborates with experts, law enforcement, and government agencies to develop a safer Internet.**

[1] Facebook is not directed at children less than 13 years of age residing in the United States and does not knowingly collect information from any children under 13 in the United States. Nevertheless we recognize and take seriously our responsibilities as a corporation to protect children and enhance the online safety of children 13 years of age and older who are our users. Accordingly, Facebook was built with the requirements of the Child Online Privacy Protection Act (COPPA) in mind. When Facebook becomes aware of accounts established by children under the age of 13 we terminate those accounts and delete all the information uploaded by that account.

- **Congress has a role to play to support and encourage, not discourage or prohibit companies' innovations to advance child and teen online safety, security and privacy.**

We request, therefore, that Congress not overhaul COPPA, but instead provide legislative and regulatory incentives to companies to innovate on child safety and privacy technologies, and prevent regulators from foreclosing innovation and experimentation in this area

Our testimony lays out in brief a number of the key innovations employed by Facebook to promote safety for teens and others online.

Facebook Innovation 1: A Real Name Culture Promotes Online Safety

Facebook's approach to providing online safety leadership begins with the recognition that there is no existing system today that can verify the age of a child online. As a result, Facebook developed and implemented an innovative, multi-layer system to act as technological proxies for age. These layers are discussed in greater detail below and are enhanced by Facebook's innovation of using a "real name" culture, which allows us to better filter out fake accounts and identify inappropriate contact.

Before Facebook, the common wisdom was that Internet users should avoid using their real names and sharing information on line. Facebook was the first major web service that required people to build their profiles and networks using real names, and provided them with privacy tools to enable them to decide who could access that information. This important policy and technical architecture decision not only allowed Facebook users to become more connected, but also made the site safer. A culture of authentic identity made Facebook less attractive to predators and other bad actors who generally do not like to use their real names or email addresses.

Facebook's real name culture also attracts users who are more likely to adhere to our Statement of Rights and Responsibilities (SRR, or what other companies call Terms of Service) and keep their behavior consistent with the standards of their communities. People are less likely to engage in negative, dangerous or criminal behavior online when their friends can see their name, their speech and the information they share. The real name culture creates accountability and deters bad behavior since Facebook users understand that their actions on our service create a record of their behavior. When users actions violate our SRR or the law, we can pinpoint corrective action – usually account termination and/or referral to law enforcement in potential criminal matters – to the specific account involved. Similarly Facebook is often able to detect fakes because of the types of connections made by a fake user account. And, of course, it's difficult to connect to friends using a fake account, since they are more likely to reject friend requests from people they do not know. Facebook also routinely blocks the registration of accounts under common fake names.

Our real name culture also empowers users to become "community policemen," and report those whose behavior violates Facebook's SRR. Facebook's users regularly use our report button, found throughout the service. This substantially multiplies the number of people reviewing content and behavior on Facebook and greatly enhances safety of teens on Facebook. At the same time, user actions often appear in the newsfeeds of his or her friends. If a friend learns of inappropriate behavior, he or she can intervene with a user to determine whether something is wrong.

FACEBOOK INNOVATION 2: USER CONTROL ON FACEBOOK ENHANCES PRIVACY AND SAFETY

Since its inception, Facebook has built innovative privacy tools for users to exercise direct control and share what they want, with whom they want, and when they want. This user control model supplements the protections designed into our service and empowers our users of all ages to protect themselves online.

Perhaps more importantly for this hearing, Facebook's user control model also allows users to determine whom they are connected with on Facebook. Facebook users must accept a request from another user to be connected - Facebook never makes that choice. If a user feels uncomfortable connecting with a particular person, she may decline that friend request. Further, if a user begins to feel that a friend on Facebook is annoying, spamming, harassing, and/or dangerous, she may de-friend that person at any time. This action of de-friending terminates the connection between the users and prevents further contact.[2] A user may also "block" another user in order to prevent any contact between the two. And, any user may at any time use our ubiquitous report button to draw Facebook's attention to inappropriate behavior.

Facebook takes its commitment to innovating to advance user privacy seriously. When new users sign up, they are introduced to our privacy help center, which explains how they may set a privacy setting for each piece of content the user shares. In December 2009, we introduced an unprecedented privacy dialog, which required every Facebook user, worldwide, to stop and consider their privacy settings before they could use the service further.   As a result of that process, an additional one-third of our users customized their privacy settings.

FACEBOOK INNOVATION 3: HIDDEN SECURITY SYSTEMS AND SAFETY TOOLS ADVANCE FACEBOOK USERS ONLINE SAFETY

Facebook's safety innovations extend to the development and use of proprietary technologies that allow us to continuously improve online safety and combat emerging online threats.   Although we do not generally discuss these publicly for fear that they may be compromised or circumvented, these technologies allow Facebook to perform ongoing authentication checks, including technical and community verifications of users' accounts.   We look

[2] It should be noted that the de-friending and blocking occurs without notification, so the connection is simply, elegantly, electronically severed without drawing attention to the ending of the connection.

for anomalous behavior in the aggregate data produced by our 400 million users. For example, if an adult sends an unusual number of friend requests to unrelated minors which are ignored or rejected, our systems could be triggered, sending up a red flag and initiating a Facebook inquiry and remedial actions.

FACEBOOK INNOVATION 4: FACEBOOK EMPLOYS AGE GATES TO LIMIT SHARING AND CONNECTIONS BETWEEN MINORS AND ADULTS

As stated earlier, Facebook is neither directed at children less than 13 years of age nor does Facebook knowingly collect information of those under 13. Our privacy policy is explicit in this regard:

> If you are under age 13, please do not attempt to register for Facebook or provide any personal information about yourself to us. If we learn that we have collected personal information from a child under age 13, we will delete that information as quickly as possible. If you believe that we might have any information from a child under age 13, please contact us through this help page.

Accordingly, Facebook is not required to comply with many of COPPA's requirements. However, Facebook actively removes accounts once discovered, of anyone it learns is under 13. It also employs a number of age gating technologies to limit the contact, sharing and connections between minors and adults. Facebook limits minors' access to the service by requiring those entering Facebook.com to type in their age on the very first screen.[3] This birth date field prohibits children under the age of 13 from establishing an account. The age gate technology places a persistent cookie on the device used to establish an account, preventing the user from attempting to modify their birth date.

Facebook further employs a separate set of age restrictions to further limit contact between minors and adults. These restrictions are intended to limit opportunities for adults to pose as minors. Facebook engages in what we call social verification to ask minors that are new to our service to consider the source of a new friend request. Along with the friend request we may interpose a question to the minor prior to the minor being able to confirm that they wish to accept that request. Typical representative questions asked of the minor: (i) Is this someone whom you know from your school?; or (ii) Is this someone whom you or your parents know from your community? We also limit the number of friend requests that anyone can send in a set period of time to further reduce unwanted contacts between unrelated users.

[3] The Subcommittee should note that many other leading online companies and social networks never even attempt to collect users' date of birth, and, therefore, never even attempt to block minors from using their sites and services.

Additional limitations further limit the sharing of data between minors and adults on Facebook. While those over 18 on Facebook can share information with everyone, Facebook automatically restricts users under 18 from doing so. Facebook automatically limits their sharing to a much smaller subset of users, such as the minor's friends, friends of those friends, and their verified networks, generally associated with their schools. This limitation substantially reduces the visibility of minors to non-minors whom they do not know.

FACE BOOK INNOVATION 5: FACEBOOK ENGAGES IN EXTENSIVE ADDITIONAL SAFETY EFFORTS TO COMBAT SPECIFIC THREATS TO TEENS ONLINE

Facebook innovations also combat specific threats to teens on our service and the company cooperates closely with law enforcement on these issues, upon receipt of appropriate legal process.

Suicide and Self-Harm

Facebook regularly delivers information to each user's networks of friends. As a result, Facebook stands in a special position to help reduce teen suicides and other forms of self-harm. Users who witness changes in their friends' behavior, reflected in their Facebook postings, can intervene to prevent friends from harming themselves. The promotion of self-harm, including eating disorders, cutting, etc., is a violation of Facebook's Statement of Rights and Responsibilities, and we encourage users to report this information. Our dedicated team of User Operations analysts reviews these reports and removes content such as photos, groups, and events. When we receive a report of someone who has posted suicidal content on Facebook, we alert the National Suicide Prevention Lifeline and encourage the user to contact his or her local authorities/law enforcement immediately. We've also posted an FAQ to the privacy and safety page in our Help Center with information and links to suicide help resources. Facebook saves lives on a regular basis by helping to prevent this kind of behavior. Our real name culture helps people identify those who are truly in need and respond in real time to a cry for help.

Cyberbullying and Harassment of Teens Online

Facebook has led efforts around the world to help combat cyberbullying. In the US, Facebook was a founding member of the Stop Cyberbullying Coalition. Our robust reporting infrastructure leverages Facebook's 400 million users to monitor and report offensive or potentially dangerous content. This infrastructure includes, systems to prioritize the most serious reports, and a trained team of reviewers who respond to reports and escalate them to law enforcement as needed. The team treats reports of harassing messages as a priority, reviewing and acting on most within 24 hours. We also prioritize serious reports submitted through the contact forms in our Safety Center. With assistance from our outside experts on our Safety Advisory Board we have produced new materials on our Safety Center that specifically address how to prevent or respond to cyberbullying. We have also partnered with other organizations like MTV on their 'A Thin Line' campaign to educate young people about the dangers of digital abuse; with the BBC on their 'bullyproof' campaign, and regularly invite experts, such as the National Crime Prevention Council to address cyberbullying on the Facebook Blog, which reaches over 8 million people.

Missing Children and Runaways

Facebook has also been successful in helping to locate missing teens. Law enforcement has generously praised Facebook for prioritizing law enforcement requests for IP location information that might help locate a missing child, which we provide on receipt of appropriate legal process. In just one week last February, we helped authorities in Fairfax, Virginia and Menlo Park, California find and return two missing kids. Last July, we received a request for IP data and basic user information for a minor who had gone missing. Over the course of the next week, we worked closely with law enforcement over email and by telephone. Ultimately, the minor was found using the exact IP data we had provided. Similarly, a Facebook user went missing in Canada, and a demand for ransom was made. The Royal Canadian Mounted Police contacted us, and we followed our procedure for imminent threats. When a message was sent to a friend from the missing person's account, we provided the necessary data, enabling the RCMP to locate and return the person to safety.

Preface: only a tiny fraction of a single percent of users will ever encounter the following two kinds of behaviors on Facebook. We focus on these areas because we take any threat to our users' safety very seriously.

Registered Sex Offenders Attempting to Establish Accounts

Although it is not required to do so by law, Facebook prohibits access to Facebook by Registered Sex Offenders (RSOs). Facebook employs an outside contractor – at our own expense – to collect a list of RSOs from all of the states periodically throughout each year. Every state and locality keeps their list of RSOs in a different file format with different information and different character fonts. etc. We periodically compare that compilation of names to our user list; we do not wait for law enforcement to request that we do so. Our internal team of investigation professionals evaluates any potential matches more fully. If we find that someone on a sex offender registry is a likely match to a user on Facebook, we notify law enforcement and disable the account. On occasion, law enforcement has asked us to leave the accounts active so that they may investigate the user further.

We have worked proactively to establish a publicly available national database of registered sex offenders that enables real-time checks and includes important information like email addresses and IM handles.

Child Pornography

Facebook takes substantial steps to stop any trafficking of child sexual exploitation materials, commonly referred to as child pornography. We use automated tools to automatically prohibit any sharing of known links (i.e. URLs) containing these materials so that these links cannot be distributed across our service. Facebook has a highly trained team dedicated to responding to the rare occasions when child pornography is detected on the service. That team sends incident reports to the National Center for Missing and Exploited Children (NCMEC) and the US Department of Justice for potential prosecution. When we encounter what we believe are new offending URLs, we deploy a new technology we have developed that enables us to pull down any URL shared throughout our service even though it has been distributed.

Facebook Innovation 6: Facebook Has Made a Commitment to Collaborate on the Advancement of Safety Online

Although Facebook has important responsibilities in advancing safety online, , Facebook recognized the importance of collaborating with others to innovate in this area. Facebook has developed deep, ongoing relationships with child safety and security experts. In December, Facebook formalized these relationships by creating a Safety Advisory Board of outside experts who advise us, and, on occasion, our users about how to keep teens safe online. Facebook also continues to work closely with law enforcement agencies around the country, and around the world. We are particularly proud of our work with the states' Attorneys General. In 2008, Facebook actively participated in the Internet Safety Technical Task Force at the behest of the Attorneys General to examine these issues. In April, we launched our new Safety Center to provide our users, parents and educators with updated educational materials and information about how to utilize our innovative privacy and security tools to enhance online safety.

Conclusion: Facebook Will Continue to Innovate But Congress Must Help

Although we are not a service that is directed at children less than 13 years of age, we have built our service, policies, and tools with COPPA in mind. Our experience tells us that Congress need not amend COPPA at this time. In fact, any amendments might undo many of our innovative privacy and safety tools. Congress can, however, assist Facebook and companies like us in advancing online child and teen safety by providing incentives, not disincentives, for child safety innovation online. If COPPA is amended, Congress could consider permitting companies to explore innovative approaches to obtaining parental consent online. Congress should ensure regulators are not discouraging technological and policy innovation in this area when reviewing privacy and security policies of companies that are trying to do the right thing.

We thank this Subcommittee for its leadership and call on Congress to take these actions to enhance child online safety. Thank you for your consideration.