Testimony of Joe Sullivan

Chief Security Officer

Facebook

July 28, 2010

Before the U.S. House of Representatives Committee on the Judiciary,

Subcommittee on Crime, Terrorism, and Homeland Security

Hearing on: Online Privacy, Social Networking, and Crime Victimization

Summary of Key Points

Promoting a Real Name Culture: Facebook's real name culture creates accountability and deters bad behavior since people using Facebook understand that their actions create a record of their behavior.

Empowering People with Privacy and Safety Controls: Facebook' mission is to give people the power to find, connect, and share information with their friends and the people around them, and we make it easy for people to decide what they want to share, with whom, and when.

Deploying Hidden Security Systems and Safety Tools: Facebook has developed and deployed proprietary technologies that allow us to continuously improve online safety and combat emerging online threats. These technologies enable Facebook to perform ongoing authentication checks, including technical and community verification of users' accounts. We also have dedicated teams responsible for investigating specific scams perpetrated against our users, and to use legal means to go after the people behind them.

Addressing Special Needs of Teens Online: We have developed a number of tools and technology innovations designed to enhance the privacy and safety of teenagers on Facebook. We have led efforts around the world to help combat cyberbullying and combat suicide and self harm, and we have built a strong track record in helping to locate missing teens. Finally, while only a tiny fraction of a single percent of users will ever encounter sexual predators or content involving child pornography on Facebook, we focus on safeguards in these areas because we take them very seriously.

Driving Collaborating Among Key Stakeholders in the Online Safety Community: We have built strong relationships with child safety and security experts, and we work closely with government and law enforcement agencies around the country, and around the world.

More Can be Done With the Help of Congress: To combat criminals and miscreants who would use the Internet to engage in scams, identity theft, and fraud:

- We need to move forward with creation of a national database of convicted sex offenders that includes online identifiers and is accessible to industry and the online safety community.

- We need renewed investment in youth and parent Internet education programs.

- We need to give internet companies broader access to hashes of known images of sexual exploitation of children.

- We need more resources to train law enforcement officers on social technologies, and they need better technology to do their job.

- We need better cooperation between law enforcement entities in different jurisdictions. Most interstate cases move too slowly, and most international cases never get prosecuted at all.

From its beginnings, Facebook sought to provide a safer environment than was generally available to people on the web, and as we have expanded beyond college students, we have worked hard to deliver a safer online experience for all of our users**.** The five hundred million people across the globe who actively use Facebook have driven innovation in ways that few would have predicted a decade ago, and Facebook will continue to innovate in order to enhance the safety and security of our thriving community.

Thank you Chairman Scott, Ranking Member Gohmert, and Subcommittee Members. My name is Joe Sullivan, and I am Facebook's Chief Security Officer. As Facebook's CSO – and also as a former federal prosecutor and a founding member of the first of the Justice Department's Computer Hacking and Intellectual Property Units, a special team created by now F.B.I. Director Robert Mueller and located in the heart of Silicon Valley, - this topic has special resonance for me. At Facebook I work to develop and promote high standards for product security, engage educators, parents, students and other Internet users externally to promote safe Internet practices. I also oversee a team that partners closely with law enforcement to help ensure that those responsible for spam, fraud and other abuse are held accountable. Facebook is constantly innovating to foster a safer online environment and to address new and emerging security threats. We believe these proactive efforts and innovations – some that are visible and others that are not – are a key to providing a positive online experience.

While the Internet now connects nearly 2 billion people around the world,[1] until recently it was a useful but passive repository of information. People visited Web sites, read articles, and gathered information, but had little if any meaningful interaction with one another on the Web. In just a few short years, however, the Internet has evolved from an impersonal, anonymous medium to an interactive social experience defined by a person's connections, interests, and communities. That transformation occurred in tandem with what has been called "Web 2.0," an explosion in innovative functionalities that was unimaginable during the Internet's infancy. These developments provide interactive experiences and allow people to generate and define relevant content. They enlist people as both the viewers *and* creators of online content, frequently in a framework that is social and involves forums or communities defined by the users themselves.

Since its creation in a Harvard dorm room by Mark Zuckerberg in 2004, Facebook has been at the forefront of this change, growing from a network of students at a handful of universities to a worldwide community in over 180 countries. As Facebook expanded, we continually innovated and implemented new tools, responding to the immense public demand for more and better ways to share and connect. Today, Facebook and other social technologies have the power to enrich people's lives—and society as a whole—in ways that were un-imagined five years ago. Facebook has become an invaluable communication tool, allowing individuals and families to connect for myriad purposes—for charitable causes, in the political realm, for grassroots organization, and for local community building.

---

1 *Internet Usage Statistics, The Internet Big Picture*, World Internet Users and Population Stats, http://www.Internetworldstats.com/stats.htm.

From the beginning, Facebook sought to provide a safer environment than was generally available to people on the web, and as we have expanded beyond college students, we have worked hard to deliver a safer online experience for all of our users.[2] We reach out to law enforcement and Internet privacy, safety, and security experts everywhere to learn about best practices and to build on them. For example, in December, we convened a Safety Advisory Board consisting of representatives from five leading online safety organizations (Childnet International, Common Sense Media, ConnectSafely.org, the Family Online Safety Institute, and WiredSafety) to provide independent advice on teen online safety. Both to share our insights and to stay fully informed, Facebook has participated in 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.

No discussion of key stakeholders in ensuring internet safety would be complete without recognizing the excellent work done by law enforcement across America. I'm proud to say that we have forged strong working relationships with the law enforcement agencies here at the table today. The FBI has long been a leader in cybercrime investigations, and is working closely with us on several large multi-jurisdictional cases right now against malware distributors and spammers who have attempted to take advantage of the scale of social networking sites. The FBI is very focused on child safety—with many agents across the country playing leadership roles in ICAC taskforces. And we have found the Secret Service to be very resourceful and innovative not only on the threat cases they prioritize but also on other types of electronic crimes investigations where we have turned to them for assistance.

Today I would like to discuss some of the important ways that Facebook innovation helps promote a safer online environment.

Summary of Key Points

I will discuss five areas in which our innovations are helping to make our site safer and deliver the best experience to the people who use Facebook:

1. **Promoting a Real Name Culture;**
2. **Empowering People with Privacy and Safety Controls;**

[2] 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.

3. **Deploying Hidden Security Systems and Safety Tools;**
4. **Addressing Special Needs of Teens Online;**
5. **Driving Collaboration Among Key Stakeholders in the Online Safety Community.**

Promoting a Real Name Culture

Before Facebook, the common wisdom was that Internet users should avoid using their real names or sharing information online. Facebook was the first major web service that required people to build their profiles and networks using real names while, at the same time, giving them privacy tools to control who could access that information. This was an important policy and technical architecture choice, which both allowed people using Facebook to become more connected and made the site safer.

A culture of authentic identity has made Facebook less attractive to predators and other bad actors who generally do not like to use their real names or email addresses. At the same time, Facebook's real name culture attracts users who are more likely to adhere to community rules, as set forth in our Statement of Rights and Responsibilities, than users of other online services. [3] 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. Our real name culture creates accountability and deters bad behavior since people using Facebook understand that their actions create a record of their behavior. When someone's actions violate our SRR or the law, we can assign corrective action – which in serious and/or potentially criminal matters usually involves account termination and/or referral to law enforcement – to the specific account involved. Similarly, Facebook is often able to detect fake user accounts because of the types of connections made by them, and we routinely block the registration of accounts under common fake names.

Our real name culture also empowers users to become "community policemen," and to report those whose behavior violates Facebook's SRR. People who use Facebook expect authentic identities and interactions, and when they encounter something different, they are quick to notice and report that behavior. They also regularly use our report links, found on nearly every page throughout the service. This substantially multiplies the number of people reviewing content and behavior on Facebook and greatly enhances safety on the service. Our robust reporting infrastructure leverages Facebook's 500

[3] Facebook's community rules are set out in our Statement of Rights and Responsibilities ("SRR"), *available at:* http://www.facebook.com/terms.php?ref=pf

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.

We recently adopted a policy, modeled on the Fair and Accurate Credit Transactions Act, to enable persons whose accounts have been compromised to access information about fraudulent activity associated with accounts opened using their identification. This makes it easier for our members to protect their identities and their reputations. When it comes to finding new ways to safeguard the people who use Facebook, we constantly strive to be ahead of the curve. Indeed, the techniques we use to safeguard people as they engage in ever-increasing numbers of financial transactions to obtain digital goods through Facebook lead the industry. We became a Level One Payment Card Industry (PCI) compliant company well before required to do so by the PCI rules. We have a team of fraud investigators on staff monitoring transactions for anomalies – for example, a purchase made from one location with a credit card from another. Now, we are forging ahead with making sure that people feel secure in doing business with our virtual currency – Facebook Credits.

Empowering People with Privacy and Safety Controls

Facebook's mission is to give people the power to find, connect, and share information with their friends and the people around them. We have learned that the more *control* people have over their information, the more comfortable they will feel about using this service. For this reason, we make it easy for people to decide what they want to share, with whom, and when. People using Facebook must accept a request from another user to be connected - Facebook never makes that choice for them. If someone feels uncomfortable connecting with a particular person, he or she may decline or ignore the friend request. Further, if someone begins to feel that a friend on Facebook is annoying, spamming, harassing, and/or troubling, she may de-friend that person at any time, which terminates the connection between the users.[4] A user may also "block" another user in order to shut off profile access and prevent any further contact. And, anyone may at any time use our ubiquitous report button to draw Facebook's attention to inappropriate behavior.

Knowledge and awareness are both key to giving people meaningful control, and we work extremely hard to make sure that Facebook users are aware of and understand the controls we provide.

[4] It should be noted that the de-friending and blocking occur without notification, so the connection is simply, elegantly, electronically severed without drawing attention to the ending of the connection. We also encourage people on Facebook to report activity that they feel may be dangerous.

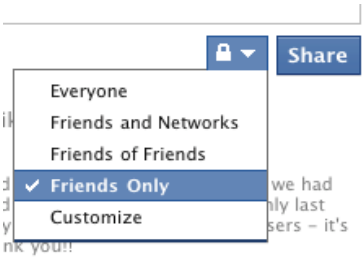
Two examples include our notice and comment process for governance of the Facebook site, and our December 2009 privacy transition tool.

Notice and Comment Process. In February 2009, we introduced an unprecedented level of user control that notifies users about proposed changes to Facebook's Statement of Rights and Responsibilities and our privacy policy – and enables them to review and comment on these changes - *before* they take effect. This process also calls for a user vote on proposed changes that trigger substantial feedback. We are aware of no other Internet-based company, large or small, that goes to such lengths to publicize and incorporate user feedback into those key documents.

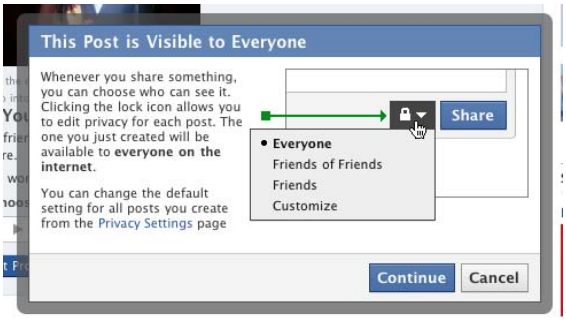
Privacy Transition Tool. Last December, when we rolled out a new privacy framework, we took the equally unprecedented step of requiring all users to navigate through a privacy transition tool to confirm or change their sharing settings. As a result, hundreds of millions of people took time to meaningfully engage with the concept of privacy and consider whether their settings reflected their preferences. No other company – on or off the Internet – has gone to such lengths to ensure that users were aware of and had a meaningful opportunity to affect their privacy choices.

As indicated above, whenever we add new features to our service we also provide additional controls so people can determine what they want to share, with whom, and when. To address increasing complexity – both with respect to the Facebook service and with respect to the privacy tools and features - last year we embarked on an effort to simplify our controls while giving people enhanced and real-time control over how they share content on Facebook. In this process we implemented several new controls, including a contextual privacy control and a one-click sharing control.

Contextual Privacy Control. We recognize that a user might want to share some information more openly (such as a comment about a world event) and other information to a narrower audience (such as a photo of their child). Our contextual privacy control allows users to control – easily, and at the time they share information - who is able to see each and every one of their posts. To exercise this control, all a user has to do is click on the "lock" icon before he or she shares the information and selects the intended audience:



We designed the tool to include a warning to make sure users are aware of what it means to share their information with "Everyone." The first time they decide to share content using that setting they see the following:



One-Click Sharing Control. To address increasing complexity, we deployed a simplified control for sharing that lets people manage over twenty categories of information with just one click. This one-click console provides more granular control to those users who prefer to customize the information they share on Facebook. This setting not only makes it easy for people to restrict the information they share in the future, it permits them to adjust the visibility of information they have shared in the past. [5]

We recently launched two additional innovative tools for helping users stay in control of their accounts. The first allows people to create a list of approved devices for Facebook logins and then to be notified immediately by both email and text message any time their account is accessed from a device not on that list. The second applies to all Facebook users. When we detect something unusual about a login attempt, we require the person logging in to verify his or her identity as the account owner before granting access. For example, if an account is typically accessed from Palo Alto, CA, and a login is attempted from Siberia, the person logging in will have to authenticate him or herself either by entering a code sent via text message or by completing a series of questions that only the account owner should be able to answer.

[5] We do not, however, make previously shared information more visible, even when someone adjusts their settings.

Developer Responsibility

We introduced Facebook Platform in 2007 to enable developers to offer innovative social experiences to people using Facebook. Since then it has given become one of the leading platforms for innovation and investment by the more than one million developers developing Facebook applications today. As Platform has evolved, we have developed more sophisticated, easier to use tools to enable people to control access to their personal information, and sharing of this information, by third-party developers: In June, we became the first platform provider to require developers to obtain "granular" data permissions before being able to access a user's information. Facebook Platform developers must tell users which specific categories of information they need to provide their application, and must obtain permission for each data category before the information can be accessed. Further, when an application provider wishes to offer users a new service, we require that the application (i) provide clear notice about any additional data it would need and (ii) obtain the user's consent. This innovative permissions model gives people more control than they have on other leading application platforms, while allowing developers to continue the vibrant innovation that has marked the Platform economy.

Deploying Hidden Security Systems and Safety Tools

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 in order to limit attempts to compromise or circumvent the safeguards, these technologies allow Facebook to perform ongoing authentication checks, including technical and community verification of users' accounts. We look for anomalous behavior in the aggregate data produced by the Facebook community and employ automated systems to block it, warn the user, and in some cases, disable the account. For example, if an adult sends an unusual number of friend requests to minors that are ignored or rejected, our systems could be triggered, sending up a red flag and initiating a Facebook inquiry and, where appropriate, remedial actions.

In addition to our technical systems and educational efforts, we have dedicated teams responsible for investigating specific scams perpetrated against our users, and to use legal means to go after the people behind them. These teams have leveraged the CAN-SPAM Act to win the two largest U.S. spam judgments in history: $873 million against Adam Guerbuez, a Montreal-based spammer, in November 2008, and $711 million against the notorious spammer Sanford Wallace in October 2009. Wallace was also referred to the US Attorney's office for criminal prosecution, which means that in addition to the judgment, he now faces possible jail time, a rare occurrence in this type of case. In fact, in

every case where we have taken legal action against a spammer, the abuse has stopped. Our aggressive approach has had a noticeable deterrent effect on would-be spammers as well, as evidenced by discussion in various online criminal forums we monitor.

Addressing Special Needs of Teens Online

As stated earlier, Facebook is neither directed at children younger than 13 years of age, nor does Facebook knowingly collect information of those under 13. While today there is no tool available to online site operators that can reliably verify the age of a user, we work hard to prevent children under 13 from establishing an account in the first place. We require those entering Facebook.com to type in their age on the very first screen, and when someone enters a birth date that that establishes his or her age to be under 13, our age gate technology blocks the registration and places a persistent cookie on the device used to establish the account, preventing subsequent attempts to circumvent the screen by modifying his or her birth date. Although this age gate deters children, we understand that it does not always prevent their registration. Providing inaccurate birth date information is a violation of our SRR, however, and we ask people to notify us if they believe we might have information from a child under 13. We created a dedicated channel for people to report accounts belonging to children under 13, and we remove these accounts when we learn of them.

While research has shown that the risks minors face online are "in most cases not significantly different than those they face offline,"[6] Facebook has developed a number of tools and technology innovations designed to enhance the privacy and safety of our teenage users, some of which provide safeguards that may not be available in the offline environment.

In addition to our COPPA-compliant age screening process designed to prevent registration by children under 13, Facebook restricts contact between adults and minors in a manner that is designed to reduce opportunities for adults to pose as minors. For example, when a minor who is new to our service sends a friend request, we might interpose a message along the lines of "Is this someone you know from

---

[6] *See*, *Enhancing Child Safety and Online Technologies: Final Report of the Internet Safety Technical Task Force to the Multi-State Working Group on Social Networking of State Attorneys General of the United States*, The Berkman Center for Law & Society at Harvard University, 2008 at 4 ("The Task Force asked a Research Advisory Board comprising leading researchers in the field to conduct a comprehensive review of relevant work in the United States to date. The Literature Review shows that the risks minors face online are complex and multifaceted and are in most cases not significantly different than those they face offline, and that as they get older, minors themselves contribute to some of the problems.")
http://cyber.law.harvard.edu/sites/cyber.law.harvard.edu/files/ISTTF_Final_Report.pdf

your school?" or "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 contact between unrelated users. While those over 18 on Facebook can share information with everyone if they choose, Facebook automatically limits the sharing of users under 18 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 that they do not know.

Similarly, Facebook has led efforts around the world to help combat cyberbullying. In the US, Facebook was a founding member of the StopCyberbullying Coalition. We regularly partner with organizations like MTV and the National Crime Prevention Council to educate our users about this important issue, and have created and distributed lists of safety tips on how to combat and report cyberbullying if it occurs on Facebook. We have also taken steps to combat suicide and self harm by encouraging users to report postings related to self-harm. We review reported postings, removing inappropriate content and alerting organizations like the National Suicide Prevention Lifeline where appropriate.

We are particularly proud of our track record in helping to locate missing teens. Law enforcement has generously praised Facebook for expediting requests for Internet Protocol ("IP") location information accompanied by appropriate legal process where it might help locate a missing child. (See attached letter from Detective Victor A. Kennedy, of the Montgomery County, Maryland Police Department.) For example, in just one week last February, we helped authorities in Fairfax, Virginia and Menlo Park, California locate two missing teens. Last July, we received a request for IP data and basic user information for a minor who had gone missing. We worked closely with law enforcement over email and by telephone, and 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. As soon as a message was sent from the missing person's account, we were able to provide data that enabled the RCMP to locate and return the person to safety. We also just recently launched a new Amber Alert program in Canada, and we are in discussions with the U.S. Department of Justice and National Center for Missing and Exploited Children to do so throughout the U.S. as well. The Amber Alert program enables law enforcement officials too easily and without cost broadcast an urgent message to the members of the community most able to help.

Finally, while only a tiny fraction of a single percent of users will ever encounter sexual predators or content involving child pornography on Facebook,[7] we focus on safeguards in these areas because we take them very seriously. For example, we prohibit access to Facebook by Registered Sex Offenders (RSOs) and employed an outside contractor to collect a list of RSOs from all of the states periodically. We regularly compare our compilation of RSO 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 someone on Facebook, we notify law enforcement and disable the account (unless law enforcement has asked us to leave an account active so that they may investigate the user further). We have also 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. We've drafted model legislation for states, and partnered with a number of state attorneys general to receive and compare against our site the Internet identifiers that they collect from the released sex offenders they supervise.

Facebook takes substantial steps to stop any trafficking in child sexual exploitation materials, commonly referred to as child pornography. We use automated tools to prohibit the sharing of known links to these materials, and we have a highly trained team dedicated to responding on those rare occasions when child pornography is detected on our site. That team sends incident reports to the National Center for Missing and Exploited Children (NCMEC) and the U.S. Department of Justice for potential prosecution.

Driving Collaborating Among Key Stakeholders in the Online Safety Community

Recognizing the importance of collaborating with others to innovate in this area, In December, Facebook formalized our longstanding relationships with child safety and security experts by creating a global Safety Advisory Board of outside experts who advise us, and, on occasion, our community about how to keep teens safe online. We also regularly consult with other experts in the field. 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 state attorneys general. In 2008, Facebook actively participated in the Internet Safety Technical Task Force at the behest of the attorneys general to examine

[7] *See, Enhancing Child Safety and Online Technologies: Final Report of the Internet Safety Technical Task Force to the Multi-State Working Group on Social Networking of State Attorneys General of the United States*, The Berkman Center for Law & Society at Harvard University, 2008 ("Social network sites are not the most common space for solicitation and unwanted exposure to problematic content, but are frequently used in peer-to-peer harassment, most likely because they are broadly adopted by minors and are used primarily to reinforce pre-existing social relations.")

these issues. In May, we announced another new partnership – with the National PTA (Parent Teacher Association), which is designed to get important educational materials to teachers, parents, and students.

In April, we launched our new Safety Center to provide teens, parents, educators, and members of the law enforcement community with updated educational materials and information about how to utilize our innovative privacy and security tools to enhance online safety. Just yesterday, we launched our Facebook Safety Page (facebook.com/FBsafety), which complements our industry-leading efforts to keep users safe on our service and elsewhere on the Web. We hope people will "like" this page to receive automatic updates in their News Feed on a range of relevant information, including new initiatives by Facebook to keep users safe, valuable educational materials from Internet safety experts, relevant news coverage and links to other online resources with important safety tips. Earlier this week, we launched a Safety Page that will complement our Safety Center to provide dynamic content to every user who "Likes" the page. Next month, for the second year in a row, I am going to be a keynote speaker at the biggest annual child safety conference, in Dallas, where we will train law enforcement and other child safety officials from around the world on best practices in doing online investigations.

MORE CAN BE DONE WITH THE HELP OF CONGRESS

Of course, Facebook cannot protect online users on its own. The involvement of the federal government is also needed, for example, to guard against criminals and miscreants who would use the Internet to engage in scams, identity theft, and fraud. That is why we applaud Congress for enacting targeted statutes to address these problems without cabining the creative freedom that is the life force of the Internet. The Computer Fraud and Abuse Act, the Child Online Privacy Protection Act, and the Controlling the Assault of Non-Solicited Pornography and Marketing Act (the "CAN-SPAM" Act) all have served to protect the public from some of the Internet's dangers and annoyances. But there is more to be done. For example:

- We need to move forward with creation of a national database of convicted sex offenders that includes online identifiers and is accessible to industry and the online safety community. . We actively supported passage of the KIDS Act, which will called for creation of just such a database, and were glad to see it signed into law (in 2008). But the Act needs to be implemented now - not some indeterminate date in the future.

- We need renewed investment in youth and parent Internet education programs. We've worked closely with private organizations on a variety of safety and security curricula, but a program taught at schools around the country and aimed at teaching kids the rules of the road would drastically reduce the number of bad incidents. Digital literacy needs to improve most

dramatically among those who have the most impact—parents and teachers- and those who are exposed to the greatest risks – students.

- We need to give internet companies broader access to hashes of known child pornography images. We report instances of child pornography to the National Center for Missing and Exploited Children whenever we find them or users bring them to our attention. With better technology, however, we could block these images upfront and identify those responsible so we can preserve information and notify law enforcement as quickly as possible. NCMEC has given us a small list, but law enforcement has access to lists that are orders of magnitude larger in volume.

- We need more resources to train law enforcement officers on social technologies, and they need better technology to do their job.

- We need better cooperation between law enforcement entities in different jurisdictions. Most interstate cases move too slowly, and most international cases never get prosecuted at all.

- Finally, Congress can assist Facebook and similar companies in advancing online safety by providing incentives for innovation and by ensuring that regulators do embrace technological and policy innovation in this area.

CONCLUSION: FACEBOOK WILL CONTINUE TO INNOVATE BUT CONGRESS MUST HELP

The five hundred million people across the globe who actively use Facebook have driven innovation in ways that few would have predicted a decade ago. The promise of this thriving community is limitless. From its beginnings, Facebook sought to provide a safer environment than was generally available to people on the web, and we will continue to innovate in order to enhance the safety and security of our thriving community.

We thank this Subcommittee for its leadership and dedication to internet innovation and safety. Thank you for your consideration.