Testimony of Bret Taylor
Chief Technology Officer
Facebook

Hearing on Consumer Privacy and Protection in the Mobile Marketplace

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

May 19, 2011

Chairman Rockefeller, Chairman Pryor, Ranking Member Toomey, and Members of the Committee, my name is Bret Taylor, and I am the Chief Technology Officer at Facebook. Thank you for inviting me to testify today on privacy issues in the mobile environment. Facebook is committed to providing innovative privacy tools that enable people to control the information they share and the connections they make through our mobile applications, as well as on facebook.com. We appreciate the Committee's initiative in holding this hearing today and providing us the opportunity to discuss our efforts to enable people to connect and share in a safe and secure environment.

The explosive growth of smartphones and mobile applications, along with innovations in the way individuals interact and share information, has brought tremendous social and economic benefits. Just a decade ago, few individuals had Internet-enabled mobile phones. Online content was largely static and consumed through desktops. When people interacted, they did so using very limited forms of communication like email and instant messaging. Today, smartphones have become indispensable devices for many people, and the technology that many of us carry in our pockets enables access to a far more personalized and interactive "social web" through which people can choose to share their experiences with friends and receive content that is tailored to them individually.

Facebook develops innovative products and services that facilitate sharing, self-expression, and connectivity. We work hard to protect individuals' privacy by giving them control over the information they share and the connections they make. For Facebook – like other providers of social technologies – getting this balance right is not only the right thing to do, but a matter of survival. Trust is the foundation of the social web, and people will go elsewhere if they lose confidence in our services. At the same time, Facebook is fundamentally about sharing, and adopting overly restrictive policies will prevent our social features from functioning in the way that individuals expect and demand. Thus, to satisfy people's expectations, we not only need to innovate to create new

protections for individuals' information; we also need to innovate to ensure that new protections do not interfere with people's freedom to share and connect. We need to continually evolve our services and the privacy safeguards included in them to respond to the feedback that we receive from the community and as required by law.

In my testimony today, I will address five topics. First, I will describe how the open architecture of the Internet has empowered the innovations of the social web and is fueling the growth of the economy. I will also explain how this open architecture presents security and privacy challenges to Internet users and the steps we and other companies have taken to address these challenges. Second, I will discuss the growing importance of mobile services at Facebook and how these innovations are driving the social web. Third, I will address the robust privacy protections that we build into facebook.com and our mobile offerings. Fourth, I will discuss the infrastructure tools that we provide in order to encourage responsible privacy practices among the independent developers who use our platform. Finally, I will explain how our efforts in advancing security and privacy online must be matched by those of other actors who likewise have an important role in safeguarding the public.

I. The Importance of the Internet's Open Architecture in Fostering Innovation

Facebook provides people with exciting, innovative and free tools for communication and sharing. In addition, through Facebook Platform, Facebook provides a set of tools that enable independent third-party developers to build applications and websites that are more social and people-centered than traditional web experiences. In both respects, Facebook seeks to build upon the openness of the Internet. The Internet has flourished as a robust zone for innovation and expression because it is an open marketplace in which ideas succeed or fail based on merit. The Department of Commerce recently noted that, "in contrast to the relatively high barriers to entry in traditional media marketplaces, the Internet offers commercial opportunities to an unusually large number of

innovators, and the rate of new service offerings and novel business models is quite high."[1] This environment is what enabled Mark Zuckerberg to launch Facebook from his college dorm room in 2004. That same innovative spirit is flourishing on Facebook Platform, which is now used by more than a million third-party developers to offer a nearly infinite variety of tools that enhance individuals' experience both on and off Facebook.

The Internet as it existed at the turn of the millennium was a relatively isolated, passive, and anonymous experience, and few individuals had the ability to access online services through their mobile phones. All visitors to a news site, for example, had the same, one-size-fits-all experience – as if each of them had purchased the same edition of the same newspaper. Thanks to the transformative effects of social technology, people today can enjoy constant connectivity, personalized content, and interactive social experiences across a range of devices. On Facebook, for example, each of the more than 500 million people who visit the site each month has a highly personalized, unique experience – one that provides updates and other content based on the information and activities that the user's own unique circle of friends have shared. The social web also creates enormous opportunities for anyone with an Internet connection to connect and share with their family, friends, and the world around them. I am proud to say that almost every United States Senator and more than 400 members of the House of Representatives, have Facebook pages that they use to reach their constituents and engage with them on matters of policy and public concern. I am equally proud to highlight that, after the recent tornadoes in the Southeast scattered irreplaceable photographs and other documents far from their owners' homes, one individual created a Facebook page that more than 100,000 people eventually connected with in order to identify and return thousands of items that might otherwise never have been recovered. Further from home, Facebook's

[1] DEP'T OF COMMERCE, COMMERCIAL DATA PRIVACY AND INNOVATION IN THE INTERNET ECONOMY: A DYNAMIC POLICY FRAMEWORK 19 (Dec. 16, 2010).

photo and video-sharing features enable members of the military to stay connected with their friends and families – to watch their children grow – despite serving thousands of miles away. And, as recent news reports reveal, people around the world have embraced Facebook and other social media as key tools for social engagement.

The social web is also an engine for jobs, innovation, investment, and economic growth. One job-listing site alone includes 31,000 Facebook-related jobs.[2] Small businesses are increasingly relying on social media to generate exposure for their companies, increase sales, and obtain new business partnerships – in a recent survey, two-thirds of small business owners "strongly agreed" that social media was important for their company.[3] The social web also creates new opportunities for businesses to inform people about their products and services, which is why many companies are now hiring individuals to strategize around social media outreach.[4] At least as important, hundreds of thousands of developers have built businesses by creating applications for the social web. To take just one example, game developer Zynga, creator of the popular Farmville game, plans to hire an additional 700 employees this year and has been valued at $7 billion.[5] And entrepreneurs have only begun to tap into the advancements in productivity and collaboration that social media makes possible, which means that the social web will continue to transform the economy for years to come.

The open architecture of the Internet makes it a phenomenal catalyst for connectivity, sharing, and economic growth. But that same openness creates technical challenges: what was secure enough for the anonymous web is not secure enough for the social web. Facebook will

---

[2] Shareen Pathak, *The Facebook Job Engine*, FINS (May 16, 2011), http://it-jobs.fins.com/Articles/SB130514803310615197/The-Facebook-Job-Engine?link=FINS_hp.

[3] Michael A. Stelzner, 2011 SOCIAL MEDIA MARKETING INDUSTRY REPORT 11, 17-18 (Apr. 2011), http://www.socialmediaexaminer.com/SocialMediaMarketingReport2011.pdf.

[4] *See, e.g.*, *Social Media Growth Creates New Job Opportunities*, HERALD & REVIEW, Jan. 4, 2011, http://www.herald-review.com/news/national/article_5a1ffb20-1811-11e0-95b5-001cc4c002e0.html.

[5] Pathak, *supra* note 3.

continue to develop new technologies that protect individuals' security and privacy on the social web, and time and again we have demonstrated our ability to move quickly to address the challenges associated with harnessing the innovation of the Internet while advancing technology in a way that makes the social experience more secure. I discuss these efforts in more detail below in Sections III and IV.

II. The Role of Mobile Services at Facebook

Over 500 million people now use Facebook's free services to connect and share their information, and more than 250 million of them do so through mobile devices. The proliferation of technology platforms means that individuals are accessing Facebook on multiple devices and in a variety of circumstances – at work, at home, at school, and on the go. Ensuring a seamless experience across all of our web and mobile presences is a tremendous engineering challenge. Whenever we roll out new features, we must consider how they will be implemented on multiple versions of our product: facebook.com, our various mobile sites, the iPhone application, the Android application, Facebook for Blackberry, and custom integrations of Facebook on other mobile devices.

Facebook has taken the lead in developing innovative privacy tools to enable individuals using Facebook through mobile devices to share and connect with the people they care about, whenever and wherever best suits them. For example, we recently launched a new version of our mobile web site, m.facebook.com, that is simpler and works with the capabilities of thousands of different phones. We also introduced 0.facebook.com as a faster and free way for people to access Facebook around the world, including in locations where connectivity is especially costly and slow. Individuals who access 0.facebook.com on the networks of our partner mobile service operators can update their status, view their News Feed, comment on posts, send and reply to messages, or write on their friends' Wall – without any data charges. Individuals only pay for data charges when they view photos or when they leave to browse other mobile sites.

Another innovation we rolled out last year was Facebook Places, a feature that allows people to share where they are and the friends they are with in real time from their mobile devices. For example, individuals attending a concert have the option of sharing their location by "checking in" to that place, which lets their friends know where they are. Individuals can also easily see if any of their friends have chosen to check in nearby. Facebook Places supplements existing sharing tools by enabling individuals to connect with each other in real time and in the real world.

A recent report by the Pew Internet & American Life Project found that two-thirds of American mobile phone users take advantage of advanced data features, such as mobile applications, email and web access, and text messages.[6] The ubiquity of mobile technology makes it easier than ever for people to tap into the social web, especially for people who may not have access to broadband but do have a mobile phone. Our own internal research shows that people who access Facebook through mobile devices are typically twice as active as other individuals. This increased attention, together with the technological ability to introduce innovative features that utilize mobile capabilities, means that mobile will play an increasingly important role in how people use Facebook and the social web more generally.

III. Facebook's Commitment to Privacy in Our Product Offerings

As we continue to develop rich services on Facebook, we are guided by our recognition that trust is the foundation of the social web. As the Commerce Department has noted, "[C]onsumer trust – the expectation that personal information that is collected will be used consistently with clearly stated purposes and protected from misuse is fundamental to commercial activities on the Internet."[7]

[6] Kristin Purcell et al., *How Mobile Devices Are Changing Community Information Environments*, PEW INTERNET & AM. LIFE PROJECT, 2 (Mar. 14, 2011), http://www.pewinternet.org/~/media/Files/Reports/2011/PIP-Local mobile survey.pdf.

[7] Commerce Report 15.

Facebook builds trust, first and foremost, through the products and services we make available on facebook.com. We understand that individuals have widely varying attitudes regarding the sharing of information on Facebook: some people want to share everything with everyone, some want to share far less and with a small audience, and most fall somewhere in between. Because each individual's privacy preferences are different, we cannot satisfy people's expectations by adopting a one-size-fits-all approach.[8] Instead, we strive to create tools and controls that enable individuals to understand how sharing works on Facebook, and to choose how broadly or narrowly they wish to share information. Our commitment to these basic concepts – understanding and control – is evidenced in five specific areas, each of which is a key focus of our business.

Privacy by Design. We have taken several steps to ensure that privacy is being considered throughout our company and products. For example, we have a Chief Privacy Counsel and other dedicated privacy professionals who are involved in and review new services and features from design through launch to ensure that privacy by design practices are incorporated into our product offerings. We also provide privacy and security training to our employees, engage in ongoing review and monitoring of the way data is handled by existing features and applications, and implement rigorous data security practices. Of course, "privacy by design" does not mean "privacy by default"; as services evolve, so do people's expectations of privacy. At Facebook, we believe that providing substantive privacy protections means building a service that allows individuals to control their own social experiences and to decide whether and how they want to share information.

Transparent Policies. Many websites' privacy policies are challenging for people to understand because they are often written for regulators and privacy advocates, not the majority of people who actually use those websites. We believe that privacy policies can and should be more

[8] *See, e.g.*, Mary Madden & Aaron Smith, *Reputation Management and Social Media*, PEW INTERNET & AM. LIFE PROJECT, 29 (May 26, 2010), http://www.pewinternet.org/Reports/2010/Reputation-Management.aspx (noting that 65% of adult individuals of social networking services have customized the privacy settings on their profile to restrict what they share).

easily understood, which is why we are currently testing a new policy that communicates about privacy in a simpler, more interactive way. We call this "Privacy Policy 2.0." It uses easy-to-understand language, presents information in a layered format so that individuals can quickly zero in on what they want, and incorporates explanatory screenshots, examples, interactive graphics, and videos throughout.

Contextual Control. In its December 2010 *Preliminary FTC Staff Report on Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Businesses and Policymakers*, the FTC emphasized that consumers should be "presented with choice about collection and sharing of their data at the time and in the context in which they are making decisions." Facebook agrees. We introduced innovative per-object sharing controls in July 2009 to give people an easy way to indicate how broadly they want to share particular pieces of information. Using the per-object sharing controls, people can designate a unique set of sharing preferences for a particular type of content (such as photos and videos posted by that individual). They can also click on a simple lock icon that appears at the time of publication if they want to customize the audience for a particular photo or video that the individual wishes to share more or less broadly.

Sophisticated Security Protections. We recently launched a variety of features that enhance people's ability to make decisions about the security of the information they provide. We are the first major site to offer individuals one-time passwords to make it safer to use public computers in places such as hotels, cafes, or airports. If people have concerns about the security of the computer they are using to access Facebook, they can request that a one-time password be texted to their mobile phones. We also enable individuals to see all of their active sessions on the site and to log out of Facebook remotely, which they may want to do if, for example, they access Facebook from a friend's computer and forget to log out. In addition, we encourage people to provide information about the devices that they commonly use to log in to Facebook, which allows them to be notified by email or text message if their account is accessed from an unapproved device so that

they can quickly secure their account. Finally, we have long used the secure HTTPS protocol whenever an individual's password or credit card information is being sent to us, and earlier this year we offered individuals the ability to experience Facebook entirely over HTTPS.

Community Engagement. We work hard to obtain feedback from the people who use Facebook, and we consider this input seriously in evaluating and improving our products and services. Indeed, Facebook's efforts to publicly engage on changes to its privacy policy or information sharing practices are virtually unparalleled in the industry. For example, when we propose changes to our privacy policy, we announce them broadly and give individuals the ability to comment on the proposed changes (unless the changes are administrative or required by law). We are the only major online service provider that allows for a vote on the changes if comments reach a pre-set threshold. Time and again, Facebook has shown itself capable of correcting course in response to individual suggestions and we will continue to be responsive to that feedback.

Taken together, these privacy practices help us build and maintain people's trust as we continue to pioneer the new social and connectivity features that people who use Facebook expect and demand. And, because mobile features are increasingly important to the Facebook community, we are leading the industry in innovating around privacy tools available through mobile devices. For example, most of the privacy settings available on the facebook.com site are also available to individuals who connect to Facebook through mobile devices. Moreover, these privacy settings are persistent regardless of how the individual chooses to share information. Changes to privacy settings made on our mobile site will remain effective when that individual accesses Facebook through the facebook.com website. This enables people to make consistent, real-time decisions about the data they share – no matter where they are or what devices they prefer to use when connecting with their friends and communities.

IV. Promoting Privacy on Facebook Platform

At Facebook, we recognize that we have a responsibility to promote people's privacy interests whenever and however they are accessing Facebook's services. We also understand that Facebook has an important role to play when independent developers build applications and websites that rely on Facebook Platform to create social, personalized experiences. We believe that the best way to build trust while enhancing the openness and connectivity of the social web is for all members of the Platform ecosystem to embrace their responsibility to be accountable to individuals for protecting privacy.

A. Overview of Facebook Platform

Although we are proud of the pathbreaking features being developed every day at Facebook, we understand that Internet innovation depends on an open architecture in which a multitude of independent developers can develop new services and expand upon existing ones. That understanding is what motivated our decision to launch Facebook Platform in 2007. The Platform functionality allows third-party developers of applications and websites to offer innovative social experiences to individuals on Facebook as well as on other locations around the Internet.

To date, developers have built more than 800,000 games, mobile applications, utilities, and other applications that integrate with the Facebook Platform. To pick just a couple of examples, the Birthday Calendar application allows individuals to track birthdays, anniversaries, and other important dates. The We Read application enables people to share book titles and book reviews with their friends. And on the charitable front, the Causes application provides an online platform for individuals and organizations to raise funds for charitable causes.

The innovation enabled by the Facebook Platform extends to the mobile web. As discussed above, people who use Facebook have the option of sharing location data so that they can tell their friends where they are, see where their friends have checked in, and discover interesting places nearby. With an individual's express permission, third-party developers can access location data to

create a variety of additional social experiences, such as a travel application that gives people the ability to see which of their friends have already been to the place they are visiting, or a conference application that makes it easy for attendees to find colleagues and connect with them.

We are proud of the fact that, in just four short years, Facebook Platform has evolved into a flourishing, open ecosystem where everybody has the opportunity to innovate in a social way. The multitude of applications and websites enabled by Facebook and available through mobile devices is a good example of our commitment to an open architecture for Facebook Platform and the benefits this brings to individuals. The features that we offer on facebook.com compete directly with third-party applications and websites that integrate with the Facebook Platform. To pick just one example, Foursquare and Gowalla are popular mobile check-in services that are similar in many respects to Facebook's own Places offering. Subjecting our products to the competitive pressures of the open marketplace helps ensure that we have strong incentives to remain on the cutting edge of innovation, which ultimately benefits the public and the economy as a whole.

B. Tools to Help People Manage Their Relationships with Developers of Applications and Websites

We recognize that the vibrant nature of Facebook Platform creates significant benefits for the public, and we also know that Facebook Platform will only continue to thrive if individuals can build safe and trusted relationships with the applications and websites that they use. Because individuals should be empowered to decide whether they want to engage with some, many, or none of these third-party developers, we have created industry-leading tools for transparency and control so that people can understand what data they are sharing and make informed decisions about the third-party applications and websites that they decide to use. We also make it easy for the Facebook community to identify and report potential areas of concern.

Control. From the time of Facebook Platform's initial launch in 2007, we have made clear to individuals that if they choose to authorize a third-party application or website, the developer will

receive information about them, and we have long required developers to obtain only the data they need to operate their application or website. In June 2010, technological innovations allowed us to offer people even more insight into and control over the actions of developers on Facebook Platform: we became the first provider to require developers to obtain "granular data permissions" before accessing individuals' information. Developers using Platform must specifically identify the information they wish to use and request permission from the individual – who retains the ultimate simple choice of whether to share his or her information with that outside developer – and Facebook has deployed technical means to ensure that developers obtain *only* the information the user has agreed to share. In addition, we make it easy for individuals to revisit their decisions about the applications and websites they have authorized in the past. Users can block applications and websites they no longer want to access their information, and they can also remove certain permissions they have previously granted. Finally, we offer a simple, global opt-out tool. With just one click in the Facebook privacy settings, individuals can opt out of Platform entirely and thereby prevent their information from being shared with any applications or websites.

Transparency. We encourage people to examine the privacy practices of the applications and websites that they use, and we offer tools so that they can easily do so. For example, developers using Platform are required to provide a link to their privacy policy when seeking individuals' permission to access information. In addition, last October, we rolled out an application dashboard to increase visibility into applications' and websites' data handling practices. This audit tool allows individuals to quickly see which applications and websites they have authorized, the permissions they have given to each application or website, and the last time that each application or website accessed their information.

Community Policing. We make it easy for individuals, employees, and developers to communicate with us if they identify a problem with a developer's privacy practices. There is a "Report Application" link on the bottom of each application page so that people can easily convey

their concerns about that particular application. Developers, who are often keenly aware of other developers' data handling practices, can and do flag potential issues as well. Our dedicated Platform Operations team, which monitors and enforces Facebook's policies with third-party developers, then follows up on the leads we receive by employing a variety of monitoring, testing, and auditing processes.

Consistent with our commitment to providing a seamless experience across all devices, we have applied these transparency and control principles to the mobile space, despite the engineering challenges associated with communicating on a smaller mobile screen. Individuals who access third-party applications through our mobile offerings are also provided with granular information about what information the application or website seeks to access and asked to specifically authorize the developer's use of that data. In addition, just two months after introducing the application dashboard on the facebook.com site, we launched a similar mobile application dashboard that allows people to see a detailed view of the information they are sharing with various applications and websites and adjust their settings while on the go.

C. Promoting Best Privacy Practices Among Independent Developers of Applications and Websites

The goal of Facebook Platform is not only to enable developers to build social applications and websites, but also to facilitate direct relationships between people and the social applications and websites they use. At the same time, we expect and require application developers who use Facebook Platform to be responsible stewards of the information they obtain. To this end, we provide clear guidance to developers about how they should protect and secure information obtained from people who use Facebook, and we also build tools to help them fulfill this responsibility.

Policies and Practices. Developers are required to abide by our Statement of Rights and Responsibilities and Platform Policies, which detail developers' responsibilities with respect to the data they obtain. For example, developers may only request the data they need to operate, must

honor individuals' requests to delete information, must provide and adhere to a privacy policy that informs individuals about how the application or website handles individual data, and must refrain from selling individuals' data or transferring it to ad networks, data brokers, and other specified entities. In addition, ad networks that developers use to serve ads on applications that run on the Facebook Platform are required to agree to our Platform Terms for Advertising Providers. Among other things, these terms require the ad networks to certify that they do not possess (and will not obtain) any user data received directly or indirectly from Facebook.

Technology Tools for Monitoring and Review. In addition to manual review of specific applications or websites, we also have a series of automated reporting and enforcement tools to quickly identify and respond to potential violations of our policies. Our platform enforcement tool aggregates and displays several metrics concerning the activities of applications and websites on Platform, including how many data requests they are sending, what types of data they are requesting, and whether there have been any complaints or spam reports. We have a separate data access tool that tracks real-time data pulls and rates and provides historical and trend information, giving us insight into applications' or websites' patterns of data access. We also monitor enforcement activity through a dashboard system, which provides a real-time view of identified issues, outstanding enforcement actions, and activity by applications and websites that are under review. These tools enable us to zero in on particular applications and websites that may not be fulfilling their responsibilities, and to work with their developers to ensure that they are taking appropriate measures to protect the information that they obtain.

Continuous Improvement. As innovation fuels further advancements in technology, we implement new tools to help make Facebook Platform a more secure and trusted environment. For example, last year we worked with Yahoo, Twitter, Google, and others to build OAuth 2.0, an open standard for authentication that improves security on the Internet. Now that OAuth 2.0 is a mature standard with broad participation across the industry, we are requiring developers on Facebook

Platform to migrate to the more secure authentication standard. Although the transition presents significant engineering challenges, we believe that this migration is important because it will ultimately result in better and more secure relationships between developers and the individuals who use the applications or websites that they build.

We provide the infrastructure tools described above in order to empower developers to act responsibly when handling individual information, and the vast majority of the applications and websites available on Facebook Platform do so. When we become aware of applications or websites that knowingly break the rules, we take aggressive action to address the policy violation. In appropriate cases, Facebook has required companies to delete data acquired via Platform or banned developers from participating on Platform altogether.

We also have procedures in place to address the possibility of inadvertent data transfers. As I noted above, the open architecture of the Internet is intended to facilitate connectivity and sharing, but that same openness makes it impossible to guarantee the security of every data transfer. We interact regularly with service providers, security experts, application developers, and other participants in the Internet ecosystem, and when we are alerted to the possibility of a security issue, we act promptly to resolve the problem. For instance, we recently responded quickly after receiving a report from Symantec that so-called "access tokens," which are provided to developers to enable them to obtain the information users have authorized them to obtain, could be inadvertently passed to third parties when developers using a legacy authentication system did not take the necessary technical step to prevent this from occurring. We immediately investigated and, although our investigation found no evidence that this issue resulted in any individual's private information being shared, we took steps – including accelerating the transition to a more secure authentication system – to address the vulnerability Symantec identified before the news became public. As this example highlights, forward-thinking solutions can be achieved when all participants in the digital ecosystem embrace their responsibility to protect individual privacy.

Like all developers who use Facebook Platform, independent developers who work to make the mobile experience more social through integration with the Facebook Platform are required to adhere to our Statement of Rights and Responsibilities and Platform Policies. In addition, we make available software development kits to developers who want to build mobile applications and websites that integrate with the Facebook Platform. Those kits provide tools that help developers build more secure experiences, by incorporating the most advanced and secure technologies available.

V. Numerous Stakeholders Have a Role to Play in Advancing Online Privacy, Safety, and Security

We recognize that Facebook has important responsibilities in advancing people's privacy, safety, and security across the site, our Platform, and the social web. At the same time, others in the ecosystem likewise play an important role in protecting individuals online and in the mobile environment. These include developers, who must establish their own relationships with individuals and live up to the expectations and trust users place in them; browser and operating systems providers, who develop the tools that people use to access the web and run software and who are perhaps best situated to combat many of the technical challenges associated with the transition from the anonymous web to the social web; and individuals, who can take security into their own hands through steps such as strong passwords and educating themselves about the practices of the developers with whom they interact.

In fact, the history of advancements in the security of the Internet itself is filled with successes achieved through all affected parties working on tough problems. One example is the development and use of secure socket layers ("SSL") to allow for secure, encrypted Internet communications and data exchanges. SSL was developed by browser vendors largely in response to public demand for a more trustworthy online experience. To realize the full potential of the Internet as a medium for sharing information, developers needed to assure people that their online

communications would be secure. The development of secure technologies has led not only to the greater connectivity that characterizes the social web but also to the explosion of e-commerce and online banking, both of which are crucial drivers of economic growth.

Another advancement that was achieved through the collective efforts of interested parties is the taming of spam email. The late 1990s and early 2000s saw email inboxes and ISP servers overrun by spam, a phenomenon that was not only annoying but also costly to service providers and the public. Although spam remains a serious problem, its worst effects largely have been mitigated through the combined efforts of technology companies' development of sophisticated filtering mechanisms; legislative and regulatory measures such as the federal CAN-SPAM Act; and the public's continuing demands for action against bad actors. Both of these examples demonstrate how concerted action by various stakeholders in the Internet ecosystem – from site designers and browser vendors to government actors and the public – can contribute to an increasingly secure online environment.

As I explained above, we at Facebook work very hard to build user trust by ensuring transparency and enhancing user control, and by creating a platform that developers can use to build social applications in a safe and secure manner. We also use our position in the industry to encourage others to play their part in building and securing the digital ecosystem. Operating systems and browsers should remain vigilant in identifying and fixing vulnerabilities that could expose data and resolve longstanding design problems inherent in the architecture of the Internet itself. Social sharing networks, including Facebook, should continuously innovate on privacy, educate their users about new privacy features, and enforce their privacy policies with respect to developers who build on social networks' platforms. Developers, in turn, should adhere to our privacy guidelines, publish information about their own data handling practices, and control third party access to individual information on their own sites or applications. People who use social sharing services like Facebook should update their passwords, take advantage of safety and security

tools and resources, and educate themselves about the policies of websites and social networks they use. And government, too, should play a role, by taking action against bad actors who threaten the trust on which the social web relies, and, through proceedings such as this hearing, by highlighting the importance of online safety, security, and privacy.

VI. Conclusion

As a facilitator of the social web, we constantly strive to develop better tools that will build trust when individuals access our services through any device. We believe that it is important to enable individuals to make the privacy decisions that are right for them, and to provide infrastructure tools that facilitate trusted relationships between individuals and third-party application developers. By doing so, we are helping to promote the trust that powers the social web while offering individuals a robust forum to communicate and share information in new and dynamic ways. And we also encourage and support the efforts of other stakeholders in building and securing the mobile and online environments that are enriching people's lives every day.

Thank you for the opportunity to testify today. I look forward to answering any questions you may have.