Commissioner Julie Brill
Federal Trade Commission
U.S.-China Internet Industry Forum
Privacy Implications of Social Media
December 7, 2011

Good morning. I am truly honored to be here today among such esteemed participants from both the U.S. and Chinese governments, as well as industry, academia and civil society. A particularly warm welcome to our visitors from China who traveled a long way to be here.

Thank you to Microsoft for inviting me to talk to you about the Federal Trade Commission's work on privacy issues and, in particular, our work in connection with social media.

When thinking about privacy and how to best protect consumers, I find it useful to take a step back and reflect on the role of culture in both our attitudes and the resulting legal structures surrounding privacy. And it is interesting to further think about whether different approaches to privacy around the world are attributable to cultural differences. As many of you know, these questions receive considerable attention in the international privacy arena.

A discussion about the influences in the United States of culture on the attitudes and laws governing privacy could begin with one of my heroes—Louis Brandeis.

Brandeis was one of our most influential Justices on the Supreme Court, serving from 1916 to 1939. And he was also one of our nation's leading thinkers about privacy. Just as we are now working to modernize our current thinking about privacy in the age of Facebook, mobile apps, geolocation information, and facial recognition technologies, Brandeis's efforts to forge some earlier, bedrock privacy principles stemmed from his concerns about technological advances that were new in his day. His famous law review article, "The Right to Privacy" successfully advocated for the creation of a tort for breach of privacy.[1] Its focal point was the then-revolutionary phenomenon of "snapshot photography" with light, mobile cameras, which allowed the press to, in his words, "overstep[ ] in every direction the obvious bounds of propriety and of decency." And in *Olmstead v United States*, where Brandeis issued his famous and influential dissent, arguing that "against the government," Americans have "the right to be let alone." In that case, Brandeis was grappling with the appropriate boundaries for the use of nascent wiretap technology.

Social media, geolocation information, and facial recognition – the new technologies we are dealing with today make snapshot photography and wiretap technology look like child's play.

As the premier agency in the United States focused on privacy policy and law enforcement, the FTC continually thinks about how today's changes in technology impact businesses and consumers. As we strive to stay on top of technological advances, particularly in social media, we have learned that advances have changed the lives of consumers forever.

[1] Samuel Warren and Louis Brandeis, *The Right to Privacy*, 4 Harvard Law Review 193, 196 (1890).

Social media has changed the way we communicate and interact with our friends and family. We share our accomplishments through social media and seek support from friends and family when going through difficult times.

Social media has also changed the way companies do business, and the way they interact with consumers. Companies reach out to us through social networking websites. They want us to "like" them, and in return they might give us a discount.

Of course, the wonders of social media have raised privacy concerns that we are addressing through our policy and law enforcement efforts. One of our biggest efforts, applicable to social media as well as all other platforms that collect and use information about consumers, is our formidable "reexamination" of how we approach privacy here in the United States. After a series of public roundtables and hundreds of written comments submitted to the agency, one year ago, in December 2010, we issued a preliminary report that proposed a new approach to privacy—a new framework.[2]

Our proposals are intended to inform policymakers, including Congress, as they develop policies and legislation governing privacy. Our proposals are also intended to guide and motivate industry to develop best practices and improved self-regulatory guidelines.

Our proposed framework has three basic components. First, we call for companies to build privacy and security protections into new products. Privacy and security simply cannot be an afterthought. Companies should consider privacy and data security at the outset, as they develop new products and services. This concept is often referred to as "Privacy by Design."

Second, we call for simplified privacy policies that consumers can actually understand. It is just not realistic to expect consumers to read and understand long complicated privacy policies. One way to simplify notice is to exempt "commonly accepted" practices from the first layers of notice, to help remove the clutter so that consumers can pay attention to those practices that really matter. And for choices to be most effective, they should be clearly and concisely described. In many instances, it is optimal for these notices to be provided at a time and in a context in which the consumer is making a decision about his or her data—a practice often referred to as "just-in-time" notice.

And third, we call for greater transparency around data collection, use and retention. Consumers should know what kind of data companies collect, and should have access to it in proportion to the sensitivity and intended use of the data.

I believe that this framework is flexible enough to allow businesses to thrive, and to offer the valuable services consumers have come to enjoy. Equally important, I believe that this framework enables companies to continue to innovate.

---

[2] *See* A Preliminary FTC Staff Report on Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Businesses and Policymakers (Dec. 1, 2010), *available at* http://www.ftc.gov/os/2010/12/101201privacyreport.pdf.

One of our most talked-about recommendations is the development of "Do Not Track" mechanisms in connection with behavioral advertising—the practice of collecting information about an individual's online activities in order to serve advertisements tailored to that individual's interests. Our vision for Do Not Track is that it would allow consumers to have some meaningful control over how their online behavioral information is used. And over whether their online behavioral information is collected in the first place.

Since the report was issued last year, we have been closely examining the more than 400 comments that we received. A follow-up report is planned and we expect that report to be issued in the coming months.

Focusing more specifically on privacy and social media, a preliminary question we need to ask is this: Isn't social media all about sharing? Don't people use social media because they want to share? They do indeed. But unless a consumer has made the choice to share information with everyone, social media should be about developing your social networks and choosing what to share and with whom. Social networks give consumers the ability to choose how much to share and with whom, and social networks need to honor these choices.

Last week, as many of you already know, the Federal Trade Commission announced its preliminary approval of a consent agreement from Facebook.[3]

Our complaint against Facebook alleges a number of deceptive or unfair practices in violation of the FTC Act. These include the 2009 changes made by Facebook so that information users had designated private became public. We also address Facebook's inaccurate and misleading disclosures relating to how much information about users apps operating on the site can access. We also allege the company was deceitful about its compliance with the U.S.-EU Safe Harbor. And we call Facebook out for promises it made but did not keep: It told users it wouldn't share information with advertisers and then did; and it agreed to take down photos and videos of users who had deleted their accounts, and then did not.

The FTC settlement with Facebook prohibits the company from misrepresenting the privacy and security settings it provides to consumers. Facebook must also obtain users' "affirmative express consent" before sharing their information in a way that exceeds their privacy settings, and block access to users' information after they delete their accounts. To make sure Facebook gives its users, in the words of Facebook's Mark Zuckerberg, "complete control over who they share with at all times," we require Facebook to implement a comprehensive privacy program that an independent auditor will monitor for 20 years.

Our enforcement action against Facebook is but our latest effort to ensure that social media honor the choices they provide to consumers. Indeed, the proposed order against Facebook is similar to the Commission's order against Google that was just finalized two months ago. Our Google order resulted from Google's roll out of its first social media product—Google Buzz. We brought an enforcement action against Google because some of the features of Buzz

[3] *In the Matter of Facebook, Inc., a corporation* FTC File No. 0923184 (2011).

violated Google's privacy policy. We believed that, contrary to Google's representations, Google provided Gmail users with ineffective options for declining or leaving the social network.[4]

We also believed that users who joined or found themselves part of the Buzz network encountered controls for limiting the sharing of personal information that were confusing and difficult to find. And we charged that Google did not adequately disclose that the identity of individuals who some users most frequently emailed would be made public by default.

Our social media enforcement efforts this year have also included Twitter. Twitter settled with the Commission over Twitter's security lapses that enabled hackers to gain administrative control of Twitter in 2009.[5] These hackers were able to send phony tweets, including one that appeared to be from the account of then-President-elect Barack Obama, offering his Twitter followers a chance to win $500 in free gasoline.

Social media is certainly all about sharing. We at the FTC recognize – and applaud – the tremendous value that social media has brought and continues to bring to the lives of consumers. However, social media is also about choice. And social media operators have a responsibility to consumers. Consumers have expectations based on what social networks say they will do with consumers' information. And social networks must honor the promises they make to consumers. Finally, as we demonstrated in our Facebook settlement, certain practices by social networks in connection with consumer information are simply unfair.

Turning to behavioral advertising, this is a topic that has gotten significant attention in our privacy "rethink," and not just with respect to children. In our privacy report, we recommend the development of Do Not Track mechanisms. Do Not Track has the potential to provide consumers with information about online data collection and use practices, and to allow consumers to make choices in connection with those practices.

Industry seems to have heard – loud and clear – our call for development of Do Not Track. In the past year, we have seen considerable progress in the development of Do Not Track mechanisms. And we have seen considerable progress in industry's willingness and interest to engage with the Federal Trade Commission on these issues.

So why do I care so much about Do Not Track? After all, isn't behavioral advertising simply about giving consumers advertising that is more relevant, which benefits consumers as well as the advertiser? And it also pays for much of the free content that benefits consumers.

From my perspective, all of this is true. And yet, there are some real harms that consumers might experience from the vast quantities of data being collected about them through behavioral advertising and through other means.

---

[4] *Google Inc., a corporation* FTC Docket No. C-4336 (Oct. 24, 2011) (consent order) *available at* http://www.ftc.gov/opa/2011/10/buzz.shtm.

[5] *Twitter, Inc.*, FTC Docket No. C-4316 (Mar. 2, 2011) (consent order), *available at* http://www.ftc.gov/opa/2010/06/twitter.shtm.

Generally, I see three types of harms that consumers may experience.

First, the collection of vast amounts of data can unintentionally—or even intentionally—include sensitive information, such as health and financial information or information about sexual orientation. The collection of sensitive information should trigger heightened protections—more robust notice and choice. It is not clear that this is happening now, although there seems to be widespread agreement that the collection of sensitive information requires more protections.

While many data collectors claim that all this information is deidentified -- essentially no foul, so no harm – I am not comforted. Researchers have shown how easy it is to take deidentified data and reassociate it with specific consumers. And a great deal of so-called non-personally identified information is linked to a specific smartphone or laptop. Given how closely these devices are now associated the each of us, data that are linked to specific devices are, for all intents and purposes, personally identifiable.

Second, a harm that we are all very familiar with occurs when there is a data breach. The more data that is collected and retained, the greater the risk when a data breach occurs. Holding on to vast stores of data flies in the face of one of the fundamental principles of "privacy by design" – data minimization. If you hold on to data you don't need, for purposes that you can't now articulate but might be able to at some point in the future, you are at much greater risk in the event of a breach. Instead, it would be wise to safely destroy that data.

Third, there are very real potential harms that might not be as feasible on a small scale, but become possible on a large scale. I'm referring to the combination of data from multiple sources, including off line and social networks. We have seen researchers and some companies pull these data points together to make predictions about consumers' future behavior. I am concerned about data that are used in place of traditional credit reports, to make predictions that become part of the basis for making determinations regarding a consumers' credit, their ability to secure housing, gainful employment, or various types of insurance.

We've seen press reports about how life insurers use consumer consumption patterns to predict life expectancy – and hence to set rates and coverage the insurers offer for insurance policies.[6] Analysts are undoubtedly working right now to identify certain Facebook or Twitter habits or activities as predictive of behaviors relevant to whether a person is a "good" or "trustworthy" employee, or is likely to pay back a loan. Might there not be a day very soon, when these analysts offer to sell information scraped from social networks to current and potential employers to be used to determine whether you'll get a job or promotion? Or to the bank where you've applied for a loan, to help it determine whether to give you the loan, and on what kind of terms?

[6] Leslie Scism, Mark Maremont, *Insurers Test Data Profiles to Identify Risky Clients*, The Wall Street Journal November 19, 2010.

It is critical that we ensure that consumers' notification rights in connection with credit reports are implemented and honored for all types of reports amassed about consumers and used for sensitive purposes, like credit, employment, housing and insurance.

I started out my talk today with a reference to Brandeis and snapshot photography to memorialize our faces forever. Our faces are unique to us and that makes them a powerful tool.

Later this week, the FTC is hosting a public workshop on facial recognition technologies.[7] We'll be examining the current state of facial recognition technology, where it's headed, and what the privacy implications are for consumers. The workshop discussions will inform our thinking as we move forward into another aspect of the brave new world surrounding privacy issues.

So with that, again, I'd like to thank Microsoft for having me today and I hope the discussions throughout the forum are productive.

[7] See http://www.ftc.gov/opa/2011/11/facefacts.shtm.