Commissioner Julie Brill
Broadband Breakfast Keynote
April 17, 2012

Thank you for that kind introduction. It's great to be here today to talk about social networking and the future of privacy.

We are a nation that loves to share. Before our children can walk or talk, we teach them to share. We believe in the therapeutic and spiritual value of sharing with doctors, support groups, congregations, and friends. So it is no wonder that we have flocked to social media, a platform built on sharing, to share everything from our birth dates to films of our child's birth. For many, and for better or worse, no thought is untweeted, no detail is left off LinkedIn, no picture is not posted, no business is not broadcast. Facebook captured this ethos in its corporate mission statement, which begins "giving people the power to share..."

And social media has certainly transformed the media industry. Gone are the days where nothing was news until Walter Cronkite reassuringly told us: "And that's the way it is". Now we often get our news updates from social media, through our friends who send us links to the articles they found most interesting that day. Newsmakers employ social media to get their messages out, from the White House official Twitter account, to protestors in the Arab Spring tweeting when they were arrested, to celebrities announcing pregnancies on Twitter.[1] And relatively obscure social media users break the most significant stories through their posts, like the resident of Abbottabad who reported the unusual sight of helicopters hovering over Osama Bin Laden's compound at the start of last year's raid.[2]

Social media has also changed the way companies do business, and the way they interact with consumers. Advertising on social media is exploding. Ad Age just reported how digital decision makers in the ad industry spend their online ad dollars. A March 2012 survey found that three-fifths of these decision makers will increase their social media ad spend over the next year, while only 4 % will decrease their spending on social platforms. On average, according to the survey, social-media advertising will make up about 27% of digital budgets over the next 12 months, compared with 22% in the previous 12 months, apparently coming at the expense of other platforms such as ad exchanges and networks.[3]

---

[1] *Celebrities Who Announce Pregnancies & Births on Twitter,* Celebrity Baby Scoop, http://celebritybabyscoop.com/2012/02/13/celebrities-who-announce-pregnancies-births-on-twitter. (visited Apr. 16, 2012).

[2] *Twitter User Unknowingly Reported Bin Laden Attach,* CNN, http://articles.cnn.com/2011-05-02/tech/osama.twitter.reports_1_bin-twitter-profile-twitter-user?_s=PM:TECH. (visited Apr. 16, 2012).

[3] *Advertisers Say What We're All Thinking: Social Media Spending is Going to Explode,* Ad Age, http://adage.com/article/digital/advertisers-thinking-social-media-spending-explode/233128/ (visited Apr. 16, 2012).

But we didn't really need a survey to tell us that advertising on social media is growing. We see it ourselves every night when we log on to see what our friends and families are doing. I just wish I didn't see so many ads offering to help me get rid of my wrinkles.

So as advertisers keep the social media space thriving, Americans can continue to engage in one of their favorite pastimes – sharing – across more borders, cultures, and people than anyone could have imagined even ten years ago. What is all the fuss, then, about privacy in this space? Aren't users voluntarily jumping into the social media stream, choosing to reveal their information, clamoring to share more and more?

I'll tell you who can answer that question: any parent who has watched in horror as her child grabs a toy from a sobbing playmate, claiming, "but he wasn't sharing." Taking is not sharing; sharing can't be forced. Many privacy problems online arise when companies forget that basic principle of the playroom.

To its credit, Facebook recognized that it forgot that principle. As Mark Zuckerberg said after we announced the FTC's preliminary approval of a consent agreement with Facebook, "We made a bunch of mistakes."[4]

Our case against Facebook alleged a number of deceptive or unfair practices in violation of Section 5 of the FTC Act. These included the 2009 changes made by Facebook so that information users had designated private became public. We also addressed disclosures that we believed were inaccurate and misleading regarding how much information about users apps operating on the site can access. And we called Facebook out for promises we believed 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.[5] 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 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.

Just six months ago, the FTC finalized a similar enforcement action against Google, arising from Google's first social media product, Google Buzz, the progenitor of GooglePlus.[6] We believed that Google did not give Gmail users good ways to stay out of or leave Buzz, in

---

[4] Mark Zuckerberg, *Our Commitment to the Facebook Community*, The Facebook Blog (Nov. 29, 2011, 9:39 AM), https://blog.facebook.com/blog.php?post=10150378701937131.

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

[6] *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.*

violation of Google's privacy policies. We also believed that users who joined, or found themselves trapped in, the Buzz network had a hard time locating or understanding controls that would allow them to limit the personal information they shared. And we charged that Google did not adequately disclose to users that the identity of individuals who users most frequently emailed could be made public by default.

Facebook and Google provide platforms for those who choose to share personal information, but they cannot make that choice for their users. Taking is not sharing.

To complete the FTC's social media enforcement trifecta, in 2010, we reached a settlement with Twitter over security lapses that enabled hackers to gain administrative control of Twitter.[7] These hackers sent phony tweets, including one that appeared to be from the account of then-President-elect Barack Obama offering his followers a chance to win $500 in free gasoline.

The FTC's experience with Facebook, Google and Twitter – as well as the many other cases we've brought involving new platforms like mobile apps, children's online services, and data brokers – led us to realize it was time to update our approach to protecting consumers' privacy. We had to take account of the vast changes in technology, the myriad new ways that consumers' information is collected and used, and the need to better communicate these new practices to consumers.

Three weeks ago, the Commission issued its report that set forth a new privacy framework.[8] Our report is the culmination of a 14-month process that included extensive input from industry, academics, consumer groups, technologists, and regulators both here and abroad.

The final framework is intended to articulate best practices for companies that collect and use consumer data, including social media companies, and of course, many other types of companies as well. These best practices can be useful to companies as they operationalize privacy and data security practices within their businesses.

The report also includes the Commission's call on Congress to consider enacting baseline privacy legislation, which will provide businesses with certainty and clear rules of the road, and will enable industry to act decisively as it continues to innovate.

There are three main components to the final framework. 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."

---

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

[8] Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers, An FTC Report (Mar. 26, 2012) *available at* http://www.ftc.gov/os/2012/03/120326privacyreport.pdf.

Second, we call for simplified choice for businesses and consumers. Consumers should be given clear and simple choices, and should have the ability to make decisions about their information at a relevant time and context.

Third, we call for greater transparency. Companies should provide more information about how they collect and use the personal information of consumers.

As one way to simplify choice, we called on industry to develop a Do Not Track mechanism. And industry has made considerable progress here – by developing browser tools and icon-and-cookie based mechanisms, by promising to make these mechanisms interoperable, and by working on some technical implementing standards. Do Not Track has the potential to provide consumers with simple and clear information about online data collection and use practices, and to allow consumers to make choices in connection with those practices.

I know that many in industry are worried that providing consumers with choices like Do Not Track will lead large numbers of consumers to opt out of tracking, which could effectively end the ability of platforms and websites to fund free services to consumers through targeted advertising. But the actual experience with providing consumers choices doesn't bear this out. Google offers its users the ability to refine the types of ads they see through its "Ad Preferences" dashboard, and it also offers its users the ability to opt out of tracking entirely. Consumers seem to appreciate knowing how Google has sized up their interests, and they overwhelmingly exercise more granular choices to adjust the ads they will see, rather than opt out. I hope and believe that we will have a more user-friendly Do Not Track system in place by the end of this year, and that industry participants will come to see that it improves the user experience by engendering greater consumer trust.

Working with the various stakeholders who are developing an easy to use, persistent and effective Do Not Track system is one of the five main action items that we at the Commission have laid out for the next year as we implement the recommendations in our privacy report.

The second main action item involves the mobile space. The Commission is calling on companies providing mobile services to work toward improved privacy protections, including the development of short, meaningful disclosures. An important component of this initiative is the FTC's new project to update its business guidance about online advertising disclosures and mobile disclosures. As part of this project, staff will host a workshop at the end of May that will address, among other issues, how to make mobile privacy disclosures short, effective, and accessible to consumers on small screens.[9] The Commission hopes that the workshop will spur further industry self-regulation in this area.

Our third action item for the coming year involves data brokers – a sector of the consumer information ecosystem that I have been concerned about for quite some time. Data brokers are largely invisible to consumers. Some offer consumers the right to access and correct information, but consumers have no idea how to find many data brokers. To address these problems, the Commission supports targeted legislation that would provide consumers with access to information about them held by a data broker. To further increase transparency, the

[9] *See* Press Release, FTC, FTC Will Host Public Workshop to Explore Advertising Disclosures in Online and Mobile Media on May 30, 2012 (Feb. 29, 2012), *available at* http://www.ftc.gov/opa/2012/02/dotcom.shtm.

Commission calls on data brokers that compile data for marketing purposes to explore creating a centralized website where data brokers could (1) identify themselves to consumers and describe how they collect and use consumer data and (2) detail the access rights and other choices they provide with respect to the consumer data they maintain.

The fourth action item relates to large platform providers, such as Internet Service Providers, operating systems, browsers, and social media that have the capability to comprehensively track consumers' online activities. The Commission recognizes the heightened privacy concerns in connection with such tracking. We recognize that comprehensive tracking can occur through different technologies. To further explore privacy and other issues related to the potential comprehensive tracking that could be employed by ISPs, operating systems, social media, mobile browsers and others, the FTC will host a public workshop in the second half of 2012.

Finally, the FTC will participate in the Department of Commerce's project to facilitate the development of sector-specific codes of conduct as articulated in the recent Administration White Paper on privacy. The Administration's White Paper also recognizes the important role that the FTC will play in enforcing any codes of conduct that come out of the multi-stakeholder process.

As you can see, we have a very full privacy enforcement and policy agenda ahead of us. Much more than we can tweet about in 140 characters. Still, we try. We too are using social media to get out our message. Following the release of our privacy report, we hosted Facebook and Twitter live chats to take questions from the public. We are even tweeting about my talk to you this morning.

And now through the old-fashioned way of sharing, I'm happy to take <u>your</u> questions.