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 social 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 tweeted, 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.0033 Tdsa7.]TJTD .5.4(s)-.4(: "And tnu)5.4(s)-rp8oples0033wor009 TD tlu TD , -.00000

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's 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 pro001(oion st social m)p14 Tw consumearsb98n/y.2(e)8 4i

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

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 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 offer 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 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 implem