Commissioner Julie Brill
Federal Trade Commission
North Carolina Law Review 2011 Symposium:
Social Networks and the Law
Privacy and Consumer Protection in Social Media
November 18, 2011

It is great to be here this morning. Thank you to the organizers of this symposium. I know you have worked very hard to put this event together.

Of course, it is wonderful to be back in Tar Heel country. You know, when I first came down to North Carolina to work in the Attorney General's office a few years ago, I was asked to "declare" who I was for. After realizing that the question had nothing to do with elections, I managed to come up with an answer that pretty much summed up my feelings: the Tar Heels are my favorite team, but I love Coach K. Of course, this answer made absolutely no one happy. And it was the answer that made everyone around me realize I was destined to wind up in Washington.

Now that I am a Commissioner at the Federal Trade Commission, I and my fellow Commissioners are tasked with running the nation's chief consumer protection agency. Our mandate is to make sure consumers are not cheated or misled in the marketplace; and to protect competition, making sure that the marketplace is offering up a wide range of goods and services at the fairest price.

Our portfolio is remarkably broad. On the competition side, we work to stop anti-competitive mergers and other problematic practices across a broad spectrum of the economy. On the consumer protection side, our priorities include combating financial scams, suing those engaged in false and deceptive advertising, and making sure that consumers don't get those unwanted telemarketing calls. We even run the national Do Not Call program, which Dave Barry calls the most popular government program since the Elvis Stamp.

One of our primary focuses is privacy and data security. As the Nation's premier privacy enforcement agency, we continually think about how changes in technology impact businesses and consumers. As we strive to stay on top of technological advances, we—like all of you—have learned that social media has changed the lives of consumers forever.

Social media has changed the way we communicate and interact with our friends and family. We can broadcast where we plan to spend the evening, post articles of interest, and find out if anyone wants to join us in volunteering at a community center next week on Thanksgiving Day.

Social media also has tremendous power. As we watched events unfold during the Arab Spring in Tunisia, Egypt and Libya, we witnessed social media becoming an important part, if not the galvanizing force, behind revolutions.

We share our accomplishments through social media and seek support from friends and family when going through difficult times. We post photos for friends and grandparents who log on each day hoping for a new photo of our kids that we laugh at, or cherish (or both). We can become friends with people whose voices we've never heard. We can reconnect with those whose voices we haven't heard since getting on the school bus as children. And we can tweet our thoughts to anyone willing to listen.

Social media has also changed the way companies do business, and the way they interact with consumers. They reach out to consumers through social networking websites. They want consumers to "like" them and in return they might give a discount. They urge consumers to follow them on Twitter to learn when the 40% off for friends and family promotion begins.

This morning I'd like to talk about some consumer protection issues that arise with respect to social media. But first, I'd like to give you an overview of what we've been thinking about at the Federal Trade Commission with respect to consumer privacy generally, as our work on privacy informs some of our efforts involving social media.

In 2009, my agency began a "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, in December 2010, the FTC staff issued a preliminary report that proposed a new approach to privacy—a new framework.[1]

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 3 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 without having to go to law school—I should add that there's nothing wrong with going to law school, considering the audience today! 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 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.

1

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

One of our most talked-about recommendations is the development of "Do Not Track" mechanisms in connection with behavioral advertising. 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 information is collected in the first place.

Now, turning to privacy and social media, a preliminary question we need to ask is this: Is this an oxymoron? Isn't social media all about sharing? Don't people use social media because they want to share? They do indeed. But even when 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.

Take Twitter, for instance. Twitter allows users to "tweet" messages to "followers." Twitter offers privacy settings through which a user can choose to designate tweets as nonpublic. Users can send "direct messages" to a specified follower so that only the person who authored the tweet and the designated recipient can view the message. Twitter users can also click a button labeled "protect my tweets" which makes those tweets private so that only approved followers can view them.

But in 2009, hackers were able to gain administrative control of Twitter. They 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. The FTC brought an enforcement action against Twitter in connection with the company's security lapses that led to these hacks.

The FTC alleged that the company failed to require strong administrative passwords and failed to suspend passwords after a reasonable number of log-in attempts. We also alleged that this failure resulted in hackers being able to use a simple automated password-guessing tool to gain administrative control of Twitter, through which the hackers could view all Twitter accounts. Essentially, we alleged that despite Twitter's representations that it keeps user information confidential, it was not taking the necessary steps to honor its promises.

Twitter settled our enforcement action.[2] Under the terms of the settlement, Twitter will be barred for 20 years from misleading consumers about the extent to which it protects the security, privacy, and confidentiality of nonpublic consumer information, including the measures it takes to honor the privacy choices made by consumers, and to prevent unauthorized access to nonpublic information. The settlement also requires the company to establish and maintain a comprehensive information security program, including independent audits every other year for 10 years.

[2] In the Matter of Twitter, Inc., FTC File No. 092-3093 (June 2010) (consent order).

Twitter is not the only social media company which has flown into our enforcement radar screen. Remember Google's roll out to Gmail users of its first social media product, called Google Buzz? Well, it certainly got a lot of "buzz" for Google — but most of it was not very flattering. We brought an enforcement action against Google because some of the features of Buzz 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.

We also believed that users who joined Buzz 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.

Google settled our enforcement action.[3] As part of the settlement order, Google must implement a comprehensive privacy program and conduct independent audits every other year for the next 20 years. Also, and critically, Google must obtain consumers' affirmative express consent for product or service enhancements that involve new sharing of previously collected data.

What these two cases demonstrate is that while social media is all about sharing, it's also about choice. Consumers have certain expectations based on what they are told will be done with their information. And social networks must honor the promises they make to consumers.

We continue to monitor the social media space for practices that impact the privacy and security of the personal information about consumers.

While protecting the personal information of all consumers is at the top of our priority list, there is one segment of the population that deserves special attention. Children. The stakes are that much higher when we're talking about the sharing of personal information about children.

The implications of COPPA in the social media context are significant. Social media operators subject to COPPA must obtain parental consent prior to the collection, use or disclosure of information about children.

The FTC has brought several COPPA enforcement actions against social media operators. In fact, we just announced a new enforcement action less than two weeks ago. The social networking website at issue in this case, skidekids.com, advertised itself as the "Facebook and Myspace for Kids."[5]

million of these children are under the age of 10.[7] More recently, danah boyd, a Microsoft

And in fact, we do recognize some of the shortcomings within COPPA. Just two months ago we proposed some changes to the rule to make it more effective.

Most significantly, the changes we are proposing would make clear that COPPA applies to new media, including the mobile space. We are proposing to expand the definition of personal information covered by COPPA to include photos, videos, and audio files containing children's images or voices. The expanded definition of personal information also addresses online behavioral advertising to children. The proposed changes would require parental notification and consent prior to compiling data on a child's online activities, or behaviorally targeting advertising to a child.

We are also proposing that the COPPA rule be modified to provide more streamlined, meaningful information to parents. In addition, we are proposing significant changes to how verifiable parental consent can be achieved.

Before leaving privacy and data security to discuss other consumer protection-related issues that we're looking at in connection with social media, I want to address another very real

endorsements and testimonials in new contexts – particularly on social networks and in blogs – that did not exist a decade ago, and that consumers still do not necessarily think of as "advertising."

It was certainly time to update the Guides to make clear how our traditional rules of the road apply to social media and other online spaces.

There are four key revisions in the Endorsement and Testimonial Guides that advertisers need to keep in mind:

First, it must be disclosed if a blogger or other endorser in social media is being paid. It has always been the law that a material connection between the endorser and the marketer must be disclosed. A material connection includes a marketer's payment to an endorser to promote the product or an ad that features an endorser who is the marketer's employee or relative. The Endorsement Guides have long required disclosure of material connection if consumers would not reasonably expect such a connection.

Second, the revised Endorsement Guides contain new examples of situations in which payments by an advertiser to a celebrity endorser must be disclosed. These include

disclosing that the reviews came from paid employees working on behalf of the game developers. We believed that this information would have been material to consumers reviewing the iTunes posts in deciding whether to buy the games.

More recently, in March 2011, a company called Legacy Learning agreed to pay the FTC $250,000 to settle charges that it used misleading online consumer reviews to tout its product—in this case a series of guitar-lesson DVDs.[12] The company used an online affiliate program to recruit affiliates to promote its courses through endorsements in articles, blog posts, and other online editorial material. In exchange, the affiliates received substantial commissions on the sale of each product resulting from referrals. The Commission alleged that the company engaged in deceptive advertising by represented that online endorsements written by affiliates reflected the views of ordinary consumers or "independent" reviewers, without clearly disclosing that the affiliates were paid for every sale they generated.

As we said when we announced the revised Guides, our well-settled truth-in-advertising principles apply to new forms of online marketing. We expect – and the law demands – the same transparency in online marketing, including through social media, as in offline marketing. We continue to monitor endorsements both in the offline and online world, including social networking sites, to determine whether marketers and endorsers are complying with the new Endorsement Guides.

Thanks very much for inviting me to speak to you today, and for listening to me.

[12] See In the Matter of Legacy Learning Systems, Inc., FTC File No. 1023055 (June 2011) (consent decree).