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 to either 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 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] *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.

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 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.

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 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.

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 Federal Trade Commission enforces the Children's Online Privacy Protection Act—COPPA.[4] Generally, COPPA imposes requirements on operators of Web sites or online services that are aimed at children under 13 years of age, or that knowingly collect personal information from children under 13. COPPA and its implementing rule require that online operators notify parents and get their permission—what the statute calls "verifiable parental consent"—before collecting, using, or disclosing personal information from children. The rule also requires that operators keep the information they collect from children secure, and prohibits them from requiring children to turn over more personal information than is reasonably necessary to participate in activities on their Web sites. The agency has brought numerous actions enforcing COPPA.

---

[3] *In the Matter of Google Inc., a corporation* FTC File No. 1023136 (2011).

[4] Children's Online Privacy Protection Act of 1998, 15 U.S.C. §§ 6501-6506 (1998); Children's Online Privacy Protection Act Rule, 16 C.F.R. Part 312 (1999).

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]

This website targets 7 to 14 year-old children and their parents as an alternative social networking site where "parents are in charge." However, in our complaint we alleged that Skid-e-kids allowed children to register their birth date, gender, username, password and email without requesting a parent's email address. And once a child had registered, they were able to upload pictures and videos, and send messages to other members, again without parental consent.

According to our complaint, Skid-e-kids made no attempt to notify the registering child's parents or obtain parental consent for the data collection. In addition, we believed the failure to notify parents contradicted the website's online privacy policy, which indicated that parents would be contacted to activate their child's account and would receive communications about the child's account and Skid-e-kids' privacy practices.

The consent order settling our charges prohibits Skid-e-kids from violating COPPA and misrepresenting practices for the collection and use of children's information. Additionally, the website operator must retain an online privacy professional or join an FTC-approved safe harbor program to oversee any COPPA-covered website he may operate.

A few years ago, the FTC settled COPPA charges against another social networking web site operator, and at the time, the penalty—$1 million—was the largest ever assessed by the FTC for a COPPA violation. This settlement was with Xanga.com and its principals. According to the FTC complaint, Xanga collected, used, and disclosed personal information from children under the age of 13 without first notifying parents and obtaining their consent. We believed that the defendants had actual knowledge they were collecting and disclosing personal information from children. The Xanga site stated that children under 13 could not join, but then allowed visitors to create Xanga accounts even if they provided a birth date indicating they were under 13. Also, Xanga failed to notify the children's parents of the social network's information practices or provide the parents with access to and control over their children's information.[6]

Some well-respected observers have recently criticized the effectiveness of COPPA in the Facebook age. As you all know, Facebook's terms of service do not allow children under the age of 13 to open an account. And yet, in May of this year Consumer Reports noted in its *State of the Net* report that 7.5 million children under the age of 13 have Facebook accounts, and 5

[5] See *U.S. v. Jones O. Godwin d/b/a skidekids.com,* No. 1:11-cv-03846-JOF (N.D. Ga. filed Nov. 8, 2011).

[6] See *U.S. v. Xanga.com, Inc.*, No. 06-CIV-6853 (SHS) (S.D. NY filed Sept. 12, 2006).

million of these children are under the age of 10.[7] More recently, danah boyd, a Microsoft researcher, and several of her co-authors announced the results of their study of 1,007 U.S. parents with children aged 10-14. The authors surveyed the extent to which these children had Facebook accounts; the extent to which their parents assisted them in setting up these accounts; and the parents' feelings and beliefs about their kids participation in Facebook and other social media. The authors found that 55% of parents of 12-year-olds report their child has a Facebook account; 82% of these parents knew when their child signed up; and 76% assisted their 12-year old in creating the account. And fully 93% of the study's parents believed that it is they – parents – who should decide whether a child can access websites and online services, rather than the company providing the service or the government.[8]

Based on this study, Ms. boyd and her coauthors conclude that COPPA, by placing additional requirements on websites that either cater to kids under age 13, or know that some of their users are under age 13, creates a context in which companies choose to restrict access to children. They further conclude that COPPA inadvertently undermines parents' ability both to make choices about allowing their children to have access to these services, and to protect their children's online data.

But I think Ms. boyd's findings lead to a different conclusion. Her research reveals that parents would in fact respond well to the notice and consent process if Facebook chose to use it. The fact that parents have been involved in assisting their young children set up Facebook accounts indicates that they are seeking to be empowered. That was the impetus behind the enactment of COPPA—to empower parents to make choices about how their children share data online.

And without COPPA, there would likely be a significant decrease in sites and services that would give parents notice and control over the collection of their children's personal information. As far as I'm concerned, and as far as the parents in this study are concerned, this would certainly not be a desirable outcome.

While I commend the researchers for gathering this important data on how parents and children are interacting with social media, I believe that the findings in fact show how COPPA remains an empowering tool to parents.

COPPA is clearly not perfect. (Very few pieces of legislation are.) I don't think the answer is to abandon it, as it is clearly providing the kind of notice and choice that parents want when it comes to their kids' online activities. Rather, if there are holes in COPPA, let's fix them, and let's develop more broad based privacy protections to provide better notice and choice to all consumers.

---

[7] Consumer Reports, *CR Survey: 7.5 Million Facebook Users are Under the Age of 13, Violating the Site's Terms,* May 10, 2011, *available at* http://pressroom.consumerreports.org/pressroom/2011/05/cr-survey-75-million-facebook-users-are-under-the-age-of-13-violating-the-sites-terms-.html.

[8] danah boyd, Eszter Hargittai, Jason Schultz, and John Palfrey, *Why Parents Help Their Children Lie to Facebook About Age: Unintended Consequences of the 'Children's Online Privacy Protection Act'* First Monday, Vol. 16, No.11, November 7, 2011.

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 will 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 and growing concern about the vast quantities of consumer data that are being collected, culled, dissected and catalogued, from such sources as social media, online behavior, geolocation, government records, and offline data. This has become the essence of today's era of "big data."

Of course there are some beneficial uses from amassing, slicing and dicing huge volumes of data. I've heard researchers discuss how health care costs can be reduced through large scale analyses made possible by big data. Other researchers have discussed how sophisticated analyses of traffic patterns and congestion can be analyzed for "smart routing," which could be designed to save consumers' time. There are many other potentially beneficial uses of information and patterns that only become visible through analysis of massive amounts of data.

But there are other uses of "big data" that cause concern.

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—including 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.

Many data collectors tell me there is no need to worry about this. All this information is deidentified — essentially no foul, so no harm. I am not assuaged. 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 — many of us sleep more closely to our cell phones than we do our spouses! — data that is linked to specific devices through UDIDs and other means 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 a company holds on to data it doesn't need, for purposes that it can't now articulate but might be able to at some point in the future, the company and its customers are at much greater risk in the event of a breach. Instead, it would be wise to safely destroy that data.

Third, just as there are real potential benefits that might not be feasible on a small scale, but become possible on a large scale, there are potential harms from 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 are using consumer consumption patterns— that is, the kind of products and services the consumer buys—to predict life expectancy, and to help set rates and coverage being offered for insurance policies.

Might there be a day when a your geolocation information — a history indicating where you have physically been over a period of time — can be purchased by your current employer or potential employers to help him make a determination about whether to offer you a job or a promotion? Or a day when the bank where you've applied for a loan obtains a list of your credit card purchases to determine the terms of your mortgage?

The Fair Credit Reporting Act contains pretty strict rules designed to protect consumers in connection with the use of traditional credit reports, where consumers have certain notification rights, as well as the right to access and correct information compiled about them.[9] It is critical that we ensure these protections are implemented and honored for all types of reports amassed about consumers and used for sensitive purposes, like credit, employment, housing and insurance.

While privacy and data security concerns are front and center in our minds as we keep a close eye on the consumer experience with social media, they are not the only consumer protection issues to which we are paying attention.

Social media has provided a new advertising and marketing platform for industry. But the truth- in-advertising principles that apply to traditional methods of advertising also apply to social media. Two years ago, the Federal Trade Commission revised its Guides on Endorsements and Testimonials in Advertising.[10] This was the first update since 1980. Needless to say, the world of advertising has changed a lot in the past 30 years. We have experienced tectonic shifts in the advertising world and its movement to the online and mobile space. Today, we see

[9] Fair Credit Reporting Act (FCRA), 15 U.S.C. § 1681 et seq.

[10] Guides Concerning the Use of Endorsements and Testimonials in Advertising, 16 C.F.R. Part 255 (2009).

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 a celebrity discussing a product in a promotional way on Twitter. Basically, if the celebrity is being paid to speak publicly about the product, and consumers would not otherwise expect that an advertiser paid for that endorsement, the payment should be disclosed.

- Third, the revised Guides now clarify that both advertisers and endorsers may be liable for failing to disclose material connections, and for false or unsubstantiated claims made through endorsements. These principles also apply in social media.

- Finally, the Guides now provide that advertisements that feature a consumer endorser – and that convey a message that the consumer's experience with the advertised product or service is "typical" – must clearly and conspicuously disclose what *other* consumers can generally expect to experience, if that is different from the featured consumer's experience. The disclaimer "Results Not Typical" no longer provide a safe harbor as it did in the past.

I believe that these revisions to the Endorsement Guides provide important new and expanded guidance to advertisers across the vast array of marketing media, including social networks and blogs. Industry should take notice of these new Guides, because we are watching.

In August 2010, the FTC brought its first enforcement action under the new Endorsements Guide. In this case, a public relations agency known as Reverb was hired to promote video games and, in exchange for its services, it often received a percentage of the sales of each game.[11] One promotional strategy the company used was having its employees pose as ordinary consumers and post positive reviews of the games at the online iTunes store – without

[11] *In the Matter of Reverb Communications, Inc., et al.* FTC File No. 0923199, *see press release, available at* http://www.ftc.gov/opa/2010/08/reverb.shtm.

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).