Commissioner Julie Brill
Federal Trade Commission
International Association of Privacy Professionals (IAPP)
Practical Privacy Series
***Privacy: A Lesson from the Playroom***
December 6, 2011

Good morning. It's great to be here and thank you to Trevor Hughes and Bob Belair for inviting me to spend some time with you this morning at the Practical Privacy Series.

I've taken "Practical" to heart. Privacy has gotten too big—I simply can't cover all of the Commission's initiatives and my own priorities in the time allotted. So, I'll be practical and cover a few of the issues that I see as critical. First I'll talk to you about privacy and social media. Then I'll raise some of my concerns about the vast quantities of information about consumers being collected—and used. Last, I'll touch on industry developments in connection with Do Not Track self-regulatory efforts.

Like last year, I come to you at the beginning of the holiday season – or as some refer to it, the season of sharing. It is a good time for America: We are a nation that loves to share. Before our children can walk or ta

sharing; sharing can't be forced. Most privacy problems online arise when companies forget that basic principle of the playroom.

Facebook certainly forgot, on numerous occasions. As Mark Zuckerberg said after we announced the FTC's preliminary approval of a consent agreement from Facebook, "We made a bunch of mistakes."[1]

The complaint alleges a number of deceptive or unfair practices in violation of Section 5 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.

Facebook provides a platform for those who choose to share personal information, but it cannot make that choice for its users. There is a reason we celebrate the 1621 shared feast between Pilgrims and the Wampanoag—and not November 1st, 1831—the day the U.S. government first pushed Native Americans, in this case the Choctaw, off their land and onto the trail of tears. Taking is not sharing.

The FTC settlement with Facebook prohibits the company from misrepresenting the privacy and security settings it provides to consumers.[2] 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.

The FTC finalized a similar enforcement action against Google, arising from Google's first social media product, Google Buzz, just two months ago.[3] We believed that Google did not give Gmail users good ways to stay out of or leave Buzz, in 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

---

[1] 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.

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

[3] *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.*

users that the identity of individuals who users most frequently emailed could be made public by default.

To complete the FTC's social media enforcement trifecta, in 2009, we reached a settlement with Twitter over security lapses that enabled hackers to gain administrative control of Twitter.[4] 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.

I'm sure I am not the only one who signed up.

There is no doubt that social media, led by Facebook and its network of over 800 million members, has changed how the world shops, socializes, markets, memorializes, protests, parties, and even practices politics. If Facebook were a country, it would supplant the United States as the third largest. But neither it—nor Twitter, nor Google, nor the next big social media platform to come down the pike—is bigger than the values and laws that unite our citizens: One of these is our fundamental right to decide what we keep private and what we share. And like so many other successful and innovative American businesses that came before the social media giants of today, these companies will only become stronger as they build into their products and processes this basic value that so

We believed, however, that Skid-e-kids allowed children to register their birth date, gender, username, password, and email without providing their 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 their parents knowing. The consent order settling our charges prohibits Skid-e-kids from violating COPPA and misrepresenting how they collect and use 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.

And whether it is a social media site or a virtual world with community forums, like another of our recent COPPA cases, COPPA is designed to empower parents to decide whether their young children shou

Ms. boyd *et. al*. conclude that the additional requirements COPPA places on websites causes many sites to decide to restrict access to kids altogether rather than put COPPA protections in place—and that inadvertently undermines parents' ability both to choose to allow their children access to these services and to protect their children's data online.

I disagree. I think Ms. boyd's research reveals that parents would respond well to the notice and consent process if Facebook chose to use it. The fact that they are involved in assisting their kids to set up Facebook accounts indicates they want what COPPA seeks to provide—the power to hold their children's hands as they learn to make choices about how to share data online. Further, without COPPA, there would likely be a significant decrease in sites and services that give parents notice and control over the collection of their children's personal information—a bad outcome as far as I'm concerned, and, it seems, as far as the parents in this study are concerned.

COPPA is not perfect. (Very few pieces of legislation are.) But the answer is not to abandon the law. Rather, if there are holes in COPPA, let's fix them.

And that is exactly the approach the FTC is taking. Just two months ago, we proposed some changes to the COPPA rule to make it more effective. I remember the exact date—September 15—because I was with many of you that day in Dallas at the IAPP Privacy Academy. Most significantly, we would make clear that the COPPA rule applies to new media, including the mobile space. We are also proposing that the rule provide more streamlined, meaningful information to parents and improve the way in which it affects verifiable parental consent. Finally, we want to expand the definition of the personal information COPPA covers to include photos, videos, and audio files containing children's images or voices and to address online behavioral advertising to children.

Behavioral advertising, and not just that targeting children, is another online phenomenon that often blurs the line between sharing and taking. Internet advertisers argue they are not cyber-stalking us with nefarious intent: they are learning about our tastes and habits in order to offer us more efficient shopping and more relevant ads. The tracking cookies that adhere to us like so many cockleburs as we march through cyberspace are collecting data, to be sure. In many cases companies will use this data to provide an expe

Third, our bits of personal data—a picture posted to Facebook here, a post on a Yahoo group there—while seemingly harmless on their own, when combined can form a startlingly complete and possible damaging profile of us. We have seen researchers and some companies pull these data points together to make predictions about consumers' future behavior—predictions that could be used to make life-changing determinations about our credit, housing, employment, and all types of insurance. For example, there have been reports in the press about how life insurers use consumer consumption patterns gleaned from online tracking to predict life expectancy—and hence to set the rates and coverage the insurers offer.

Why couldn't geolocation information—a history indicating where a consumer has physically been over a period of time—be obtained by a current or potential employer to determine who he will hire or promote? Or a bank deciding on a loan application and its terms? Consumers have certain notification rights attached to traditional credit reports as well as the right to access and correct information compiled about them. We need to ensure the same safeguards are in place for all sorts of reports on consumers – gathered from any source and used for sensitive purposes, like credit, employment, housing and insurance.

If you are like most, you'll be doing a lot of sharing over the next few weeks—meals with friends and family, a little of your time and relative wealth with the local soup kitchen, memories of seasons past with