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 talk, we admonish them to share. We believe in the therapeutic and spiritual value of sharing with doctors, support groups, congregations, and friends. One of our most beloved national holidays, Thanksgiving, is rooted in a celebration of sharing: In 1621, the Plymouth Pilgrims shared their bountiful harvest with the Wampanoag tribe, the Native Americans who had turned the Pilgrims' famine into feast by sharing seeds and farming methods.

Even the "Occupy Wall Street" movement has its roots in sharing, or the lack thereof on the part of the one percent.

So it is no surprise that Americans have swarmed to social media, a platform built on sharing, to share everything from their birth date to films of their 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..."

Americans love to share, and social media lets them, across more borders, cultures, and people than anyone could have imagined even ten years ago. What is all the fuss, then, about privacy? 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. 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 many Americans hold dear.

It is exactly because exercising the choice to share is so fundamental that we seek to instill it in our children from an early age. Say hello to your Aunt Agnes, but don't talk to strangers. Share your candy bar with your sister but don't take candy from someone you don't know… unless, of course, it is Halloween and the stranger is dressed as a psycho-killer, then it is fine. Parents want to hold their children's hands as they teach them to walk that line between sharing enough but not too much.

The Children's Online Privacy Protection Act – which requires certain social networks and website operators to obtain parental consent prior to the collection, use, or disclosure of information about children – helps keep this connection between parents and our children tight as our kids navigate cyberspace.[5] The FTC has brought several enforcement actions under COPPA, the latest involving a social networking website, skidekids.com, that advertised itself to 7 to 14 year-old children and their parents as the "Facebook and Myspace for Kids"—an alternative social networking site where "parents are in charge."[6]

---

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

[5] 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).

[6] 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).

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 should be sharing their information. In May of this year, the Commission reached a settlement with Playdom, a developer of online virtual worlds, many of which cater to children.[7] Among other features, these online virtual worlds enabled children to participate in online community forums. The Commission charged Playdom with collecting and disclosing personal information obtained from children—information which included their names, email addresses, instant messenger IDs, and even their locations—all without parental consent. Hundreds of thousands of children had registered on Playdom's various sites and exposed their personal, private information without their parent's knowledge. The Commission's settlement with Playdom—$3 million in civil penalties—set a new high water mark for COPPA.

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—and 5 million under the age of 10—have Facebook accounts.[8]

Further, Microsoft researcher danah boyd and several co-authors recently announced the results of their study of about 1,000 U.S. parents with children aged 10-14. 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. Fully 93% of the parents studied believed that they—parents—should decide whether a child can access websites and online services—not the company providing the service or the government.[9]

---

[7] *United States v. Playdom, Inc*., No. SA CV-11-00724 (C.D. Cal., May 24, 2011) (consent decree).

[8] 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.

[9] 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.

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 experience most of us enjoy—data we may want to share if we had a choice.

If we had a choice: these are the key words. And the FTC, beginning with our preliminary privacy report released last December, seeks to excise that "if"—to establish a robust Do Not Track mechanism that gives consumers real choices and information about how their browsing data is collected, stored, and used.[10]

[10] *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.

Industry seems to have heard our call for Do Not Track, loud and clear. In the past year, they have been willing to engage with the FTC on building Do Not Track mechanisms and have made progress toward doing just that. I have met with many individuals and companies, both from the Digital Advertising Alliance AboutAds program and the browser firms, and we have had meaningful and frank dialogue that I hope that will continue. As these discussions go on, I am keeping my eye on several issues:

First, we need to speak the same language. We all agree that Do Not Track mechanisms should enable consumers to make a choice about being tracked online, but we don't all mean the same thing when we use the word "tracked." Our lexicon must be clear about exactly what companies can and cannot do with information about a consumer who has chosen not to be "tracked"—and that includes understanding both how data is collected and how it is used once collected.

And as long as we are penning a dictionary, we need to define "commonly accepted practices." There are practices commonly accepted in the industry that would seem uncommon, or even unknown, to the consumers who must be the ultimate measure. A Do Not Track mechanism should exempt as "commonly accepted" only those practices that are commonly understood by consumers to be part of the transaction they are agreeing to, such as collecting and sharing addresses for the purposes of shipping products. Consumers must be given a choice for other uses that they do not commonly accept.

The technology supporting Do Not Track mechanisms is critical: It has to ensure that the choices consumers make are honored. In this era, code is conduct. Technological barriers—whether arising from flash cookies, supercookies, or complex interfaces that break down so often they frustrate consumers—have to be knocked out of the way of effective consumer choice.

Finally, the success of any particular Do Not Track program hinges on a critical mass of industry players – including advertisers and ad networks – participating and fully honoring the choices that consumers make. Add to that easy-to-find and -use notices and choices for consumers, and we will have a system in place based on data consumers willingly share—rather than data companies surreptitiously swipe.

Two types of Do Not Track mechanisms are emerging: browser-based and icon and cookie-based. The concerns I just outlined apply with equal force to both. But there is another issue I am watching: how well these two mechanisms play together in the sandbox. I believe developers of each mechanism should move quickly to make sure that the user's choice will be honored, no matter which mechanism was used to express that choice.

Of course, it is going to take more than a great standard with lots of industry buy-in to set Do Not Track truly humming. Speaking as someone with 20-plus years in law enforcement, I know that the FTC will always have an important role policing the promises companies make under Do Not Track.

We've already brought enforcement actions against companies that failed to honor commitments made to consumers in connection with behavioral advertising. In early November, we announced that an ad network engaging in behavioral advertising settled FTC charges that it falsely claimed consumers could opt out of receiving targeted ads by changing their browser settings to block cookies. But the company—ScanScout—used Flash cookies, which browser settings could not block. The proposed settlement says that ScanScout has to tell the truth about how it collects consumer data and what options consumers have for controlling that; the company must also provide, and fully explain, a user-friendly mechanism that really allows consumers to withdraw from tracking.[11]

Again it all boils down to the tenet of the toddler room: share, don't take.

There are those—certainly not preschool teachers—that may roll their eyes at this. Why all the effort—working groups, standards groups, enforcement – to safeguard data about our browsing habits that many—maybe most—of us would surrender willingly, especially if it means we get to see Zappos.com ads for the perfect pair of black boots rather than pitches for the latest fad diet, especially if that allows us to continue to watch cute zoo babies for free online.

The answer is, once we have lost control of our data—without the chance to understand how it is collected or control how it is used—we may face serious threats. I'll outline three real concerns of mine.

First, when so much data is gathered about us from so many sources, intentionally or unintentionally, sensitive information about our health, finances, sexual orientation, or other intensely private matters gets swept into the bin. There is no such thing as TMI in cyberspace. And while many data collectors claim that all this information is deidentified—essentially no harm, no foul—research has shown how easy it is to take deidentified data and reassociate it with specific consumers. Further, a great deal of so-called non-personally identified information is linked to a specific smartphone or laptop, devices that are these days closely associated with each of us—many of us sleep closer to our cell phones than we do our spouses (information about me, by the way, I hope my cell phone provider is not storing somewhere in the cloud). Data that is linked to specific devices through UDIDs and other means is, for all intents and purposes, personally identifiable.

Second, the more data that is collected and retained, the greater the risk when a data breach occurs: the little Dutch boy would not have had to stick his finger in that dike if only a trickle lay behind it. Holding on to vast stores of data—much without a specific purpose—flies in the face of one of the fundamental principles of "privacy by design"—data minimization. The less free-floating data on the other side when that levee crashes down, the less chance of lasting damage to the consumers in the flood zone.

[11] *See* In the Matter of ScanScout, FTC File No. 1023185 (Nov 2011) (consent order).

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 your kids—each a part of yourself, freely given. To the extent the awesome power of the Internet, social media, and mobile technology make this sort of sharing easier and more prevalent, they are welcome additions to this happy season. To the extent, though, they allow companies to cross that border between sharing and taking, they become the unreformed Grinches, dangers to consumers and the thriving internet marketplace.

I started out my remarks today saying I'd be practical, but while I've got the podium, I'll end with shameless promotion.

On Thursday, the FTC is hosting a workshop on facial recognition, and I encourage you all to attend it you can, or watch via webcast.[12] We will be examining the use of facial recognition technology and related privacy and security concerns. We have a fantastic line up of policy makers, academics, privacy advocates and industry representatives. I won't reveal too much more—you'll have to attend or watch.

Thank you again to the IAPP for inviting me today. There's a terrific agenda today so I'll let you get to work.

[12] See http://www.ftc.gov/opa/2011/11/facefacts.shtm.