Symposium On Usable Privacy and Security
Remarks of Commissioner Julie Brill
Washington, DC
July 12, 2012

Good morning. Thanks much to Lorrie Cranor for inviting me today. I'm delighted to be here to talk to you about the Federal Trade Commission's work on privacy and data security, and our increasing emphasis on ensuring that the mobile space is a trusted environment for consumers.

Not too long ago, Commissioners at the Federal Trade Commission were talking about ensuring that the online marketplace was a trusted destination for consumers.

In some areas—like the "fine print" with respect to the terms of an offer for a product or service—we worked to ensure that disclosures are as effective in the online space as they are in the "snail mail" and "bricks and mortar" space.

In other areas, like privacy and data security, the online marketplace has resulted in concerns of a much greater magnitude than in the bricks and mortar shopping days of earlier generations.

In the online environment, the quantity and breadth of personal information collected about consumers and maintained by a wide variety of entities creates data security concerns that simply did not exist in years past.

And the amount of personal information, coupled with the ability to discern personal characteristics about consumers through analytics and other tools, also results in privacy concerns that, again, simply did not exist in years past.

For instance, we have learned that retailers like Target are able to predict with considerable accuracy whether their female shoppers are pregnant, based upon an analysis of their purchases of innocuous items like hand lotion.[1] That might enable Target to sell more cribs, but there may be some implications of that predictive capability that we as a society need to think more deeply about: What might Target do with that information? Who else can have it? And what use limitations should we place on others who might obtain this information?

In the mobile environment, these issues are of equal—if not greater—concern.

[1] Charles Duhigg, *How Companies Learn Your Secrets*, N.Y. Times, Feb 19, 2012, *available at* http://www.nytimes.com/2012/02/19/magazine/shopping-habits.html?pagewanted=all.

In an effort to address how the changing technological landscape, including the increasing reliance on mobile devices, affects our approach to privacy, in March 2012 the Commission issued a major report that sets forth a new privacy framework.[2]

It was the culmination of a 14-month process that included extensive input from industry, academics, consumer groups, technologists, and regulators both here and abroad.

The final framework is intended to articulate best practices for companies that collect and use consumer data, including social media companies, app developers and of course, many other types of companies as well.

These best practices can be useful to companies as they operationalize privacy and data security practices within their businesses.

The report also includes the Commission's call on Congress to consider enacting baseline privacy legislation, which will provide businesses with certainty and clear rules of the road, and will enable industry to act decisively as it continues to innovate.

There are three main components to the final framework. 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 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. I'll come back to this.

Third, we call for greater transparency. Companies should provide more information about how they collect and use the personal information of consumers.

While we recognize the benefits of certain online data collection, including more relevant advertising and free online content that consumers have come to expect and enjoy, we have concerns that too many consumers either do not understand they are trading their privacy for free online content or have not made an informed choice to do so.

One way to further greater choice and transparency with respect to data collection and use is through Do Not Track. The Commission called for industry to develop Do Not Track systems, which would serve as universal, one-stop mechanisms to enable consumers to control the tracking of their online behavior activities across websites.

We have stated that an acceptable Do Not Track mechanism will satisfy five critical criteria:

---

[2] Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers, An FTC Report (Mar. 26, 2012) *available at* http://www.ftc.gov/os/2012/03/120326privacyreport.pdf.

- It should be universal, covering all would-be trackers, and thus not requiring consumers to opt out repeatedly on different sites.

- It should be easy for consumers to find, understand and use.

- It should be persistent: the choice should not go away if cookies are deleted, for example.

- It should be effective and enforceable: it should not permit technical loopholes and compliance should be measured and enforced.

- Finally, it should address collection and not just the delivery of targeted ads.

Industry is making considerable progress developing Do Not Track solutions. Some are browser based solutions, and one solution that has wide support within the advertising industry is an icon-based system. Additionally, an Internet Standards Organization, the W3C,[3] is working to develop technical standards in connection with Do Not Track that would facilitate a common understanding among all stakeholders, both here and in Europe, as to how an effective system would operate.

Do Not Track should apply both in the online world and in the mobile space, giving consumers in both ecosystems the ability to make choices about how their behavior across websites is collected and used. Increased transparency through tools like Do Not Track is critical to furthering our goal of ensuring that the mobile space is a trusted environment.

And although I'm the last holdout—my phone is not very smart and it's becoming dumber by the day—I know that consumers are increasingly turning to mobile. For everything. Shopping, payments, and of course, for engaging with friends on social media, for playing games, and everything else too. Whatever you want to do, there's likely "an app for that."

Many of our favorite online shopping destinations have apps. Our banks have apps. Movie tickets, dating, just about anything you want to do, you can do it through an app. There are even apps designed to provide the user with motivation. There's an app that allows you to bet whether other folks will make it to the gym. And whether you will, too. If you don't work out, you have to pay up. If you do work up a sweat, you'll earn some bucks if others skip out.

And if, instead of working out, you're eating too much fast food, there's an app that provides you with incentive to change your ways by transforming your photo into what you will look like if you continue to eat too few salads and fail to exercise.

The demographics of those who are turning increasingly to apps are interesting as well. About 40 percent of people in households earning less than $30,000 say they go online mostly

[3] The World Wide Web Consortium (W3C) is an international community whose "mission is to lead the World Wide Web to its full potential by developing protocols and guidelines that ensure the long-term growth of the Web." *See* www.w3.org/Consortium/mission.html.

through their phones, compared with just 17 percent of those earning more than $50,000.[4] Half of African-American cellphone internet users and 40% of Latino cellphone internet users do most of their online browsing on their phones.[5]

Given the rising popularity of mobile, it is critical that we translate our long-standing consumer protection principles into the mobile space.

For example, clear and conspicuous disclosures have always been at the core of consumer protection and privacy concerns. In the mobile space, because physical real estate is at a premium, effective disclosures face considerable challenges.

At the Federal Trade Commission we have been looking at how to convey necessary disclosures to consumers. An important component of this initiative is the FTC's work to update its business guidance concerning online and mobile disclosures.

As part of this project, we hosted a workshop at the end of May that focused on how to make mobile disclosures short, effective, and accessible to consumers on small screens.[6]

We explored how icons and other signals might be part of the answer. We've learned that context is really critical. That is, it is just as important to consider when consumers are provided with critical information, and the context in which they are provided the information, as it is to consider what they are told.

So, for example, if you are about to purchase a coupon that will allow you to "buy one entrée and get another one free", it is important to know the geographic limitations to the offer. While the limitations of the offer may not fit on the initial screen that displays the coupon, the limitations of the offer would certainly need to be disclosed before you make the purchase.

With respect to privacy, if an app wants to collect your location information, it's far easier to understand why such data collection might be necessary when the service consumers have signed up for requires that information. For example, if I pay my bills online, I might download my bank's app, and a request to collect my location information when I download the app might be puzzling. But if when I'm out of cash the app allows me to find the bank's closest ATM, and if as I'm searching the app says to me "we need your location information in order to help you out here" —a disclosure in that context would make more sense and would allow me to make a more informed choice.

---

[4] Pew Internet & American Life Project, *Digital differences: While increased internet adoption and the rise of mobile connectivity have reduced many gaps in technology access over the past decade, for some groups digital disparities still remain*, Pew Research Center (Apr. 13, 2012) *available at* http://pewinternet.org/~/media//Files/Reports/2012/PIP_Digital_differences_041312.pdf.

[5] Pew Internet & American Life Project, *Cell Internet Use 2012*, Pew Research Center (June 26, 2012) *available at* http://pewinternet.org/Reports/2012/Cell-Internet-Use-2012/Key-Findings.aspx.

[6] FTC Workshop, *In Short Advertising & Privacy Disclosures in a Digital World*, *available at* http://www.ftc.gov/bcp/workshops/inshort/index.shtml.

The mobile ecosystem raises some additional challenges because of all the players involved in data collection and use—mobile carriers, device makers, platform developers, app store operators, app developers, ad services, and so on.

We need to pay close attention so that privacy will not "fall through the cracks"—we can't have a situation where each of these players assumes that someone else is taking care of providing consumers with information about how data is collected and used, and how consumers can exercise choice over these issues. Indeed, consumers expect the industry to develop clear rules of the road regarding responsibility for privacy notice and choice among the various players in the mobile space.

At the FTC, we are working with stakeholders to ensure that privacy and data security do not fall through the cracks.

And we are fully engaged in ensuring that the rules of the mobile road that we do have are obeyed through our enforcement work involving mobile issues.

In one case, a peer to peer network app included default settings that, immediately upon installation and set-up, allowed the app to publicly share users' photos, videos, documents, and other files stored on the users' mobile devices. We charged that this widespread, undisclosed sharing was unfair.

Another case involved children's apps—these were games for kids that allowed children to play the "classics," like "Cootie Catcher" and "Truth or Dare". The operator collected personal information about children, but failed to obtain their parents' permission as required by the Children's Online Privacy Protection Act.[7]

And then there were the mobile apps that claimed to treat acne with colored lights emitted from smartphones. Consumers were told to hold the screen next to the area of skin they wanted to "treat" for a few minutes daily while the app was activated. We alleged that these app operators were deceiving consumers.

And we have warned apps that provide detailed profiles about consumers to potential employers, based on information scraped from social networks, that the Fair Credit Reporting Act may apply to their activities and they should bring themselves into compliance.[8]

Yet there is much work to be done to fill in other critical rules of the road in the mobile space. The Department of Commerce is convening a multi-stakeholder process today[9] to begin

---

[7] Children's Online Privacy Protection Act of 1998, 15 U.S.C. §§ 6501-6506 (1998).

[8] 15 U.S.C. § 1681s(a)(2)(A).

[9] Meeting Notice, 77 Fed. Reg. 38597 (June 28, 2012). **http://www.ntia.doc.gov/files/ntia/publications/07122012_privacy_meeting.pdf**

developing codes of conduct regarding how companies that provide apps and interactive services for mobile devices collect and use personal data, and how they inform consumers about these practices.

Although mobile is exciting, and feels different—it is in the palm of our hands after all—mobile doesn't change everything. The mobile world faces many of the same challenges that we have seen in the world of desktop computing.

Once we peel away the jargon and get down to a deeper technical level, a mobile device is just a small computer. We should strive to take the best aspects of the desktop ecosystem and adapt them to mobile. I think the conversations taking place today—here, across town, and around the country—are important steps towards addressing these critical issues.

And if during these conversations we can reorient developers, programmers, and others in industry away from the notion that there are tradeoffs between privacy and functionality, and to think more about developing great functionality and great privacy at the same time—we will have traveled a good distance down the road towards creating a trusted environment in which consumers feel safe and industry can provide the wonderful products and services that consumers want.

Thank you.