Remarks of Commissioner Julie Brill
Before the Executive Committee of the CTIA – The Wireless Association
Washington, DC
June 7, 2011

Good morning. Thank you for having me today. Special thanks to Maureen Ohlhausen for providing me with the opportunity to spend some time with you this morning.

I know that you all have a busy agenda today, so I will get straight to the point. I would need a calculator, or better yet, a smartphone, to calculate the revenues generated from mobile apps. We are able to accomplish more and more on mobile devices; our smartphones, our tablets, our notebook computers, and more. We can send email, read a book, browse the web, text, shop, play games, pay a bill, get directions…the list goes on and on. Although they can't make a cup of coffee, you can use your smartphone to pay for one.

There is no mistaking the benefits of these capabilities. And there is no ignoring the consumer protection concerns that go along with them. Among them are privacy issues, advertising misrepresentations, fraud, and unauthorized charges. At the Federal Trade Commission we are thinking about all of these issues and we are taking action.

Let me back up for a minute. You can't take any action without the proper tools. In this case, the most important tool is a deep understanding of how all this technology works. That's why at the FTC, we have come to realize that while lawyers can do many things, there are others out there that are better equipped to closely examine what these devices are in fact doing and what they are capable of. As many of you know, we have our first Chief Technologist, Ed Felten, whom I imagine some of you know. We also have other technologists on staff who are invaluable in enabling us to make sense of it all.

That being said, I'll turn to some issues relating to privacy in the mobile space, and highlight the areas that have caught our attention.

The capability of smart phones to facilitate the collection of data and the sharing of that data is tremendous. News reports in recent months have discussed the data collection by smartphones and their apps. Calling patterns, proximity to colleagues, friends and family, and myriad other bits of information form patterns that allow scientists and others to predict patterns of diseases and illnesses, of change in political beliefs, and even of the rise and fall in the stock market. The unique identifier associated with a particular device could be used to follow an individual consumer's every move, and even perhaps predict their next move. Smart phones have the capability to facilitate the sharing of consumer information with so many entities: wireless providers, mobile operating system providers, handset manufacturers, app developers, and analytics companies, and of course, advertisers. Consumers are concerned about this. I am, too. Over the past several months, I have called on all industry players to do a better job protecting privacy in the online and mobile ecosystems. No pointing fingers, just take responsibility, and take it seriously.

As you know, the FTC is in the midst of rethinking the appropriate framework for privacy, including in the mobile space. We released a preliminary staff privacy report back in December of 2010.[1] The staff is now looking at the many comments received in response to the draft—including the CTIA submission. We expect a final report to be issued in the coming months.

At the mobile device panel during one of the FTC Roundtables[2] that preceded the report, there were two main take-aways. Neither will surprise you.

The first is that data collection through mobile devices is complex.

And the second is that the disclosures on mobile devices, if they are in fact there, are not adequately informing consumers about what information is being collected and how it is being used.

In its preliminary report, the FTC staff makes several recommendations. I'll mention a few that have special application to the mobile world.

First, "privacy by design." Build privacy into a product. Privacy is not something to be added on later. It's an essential component. In the mobile space, we'd expect to see a "privacy by design" approach that would result in only collecting personal information about consumers that is necessary to provide a requested service or transaction. Collecting more information than that creates a risk. That is hardly "privacy by design." For example, an app that can tell me to avoid certain highways because of road work doesn't need my list of contacts.

Second, with respect to sensitive information, companies should obtain affirmative express consent before collecting or sharing sensitive information, such as precise location data. In other words, create an opt-in.

Third, the report proposed a number of measures that companies should take to make their data practices more transparent to consumers, including streamlining their privacy disclosures to consumers. In the app world, this is really critical. The Future of Privacy Forum recently analyzed the top 30 paid mobile apps across the leading operating systems and found that out of those 30, 22 of them did not have a basic privacy policy.[3] That's nearly three-quarters—and I didn't even need a smartphone to figure out that percentage.

---

[1] Fed. Trade Comm'n, *Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Businesses and Policymakers* (2010) (preliminary FTC staff report), *available at* http://www.ftc.gov/os/2010/12/101201privacyreport.pdf.

[2] Fed. Trade Comm'n, "Exploring Privacy: A Roundtable Series" (2010) (press releases, agendas, and comments), *available at* http://www.ftc.gov/bcp/workshops/privacyroundtables/index.shtml.

[3] Shaun Dakin and Shreya Vora, "FPF Finds Nearly Three-Quarters of most Downloaded Mobile Apps Lack a Privacy Policy." *Available at* http://www.futureofprivacy.org/2011/05/12/fpf-finds-nearly-three-quarters-of-most-downloaded-mobile-apps-lack-a-privacy-policy/.

In the behavioral advertising area, the staff recommended implementation of Do Not Track.[4] As you know, this is a catchy name for an easy to use choice mechanism for consumers to opt out of the collection of information about their online behavior for targeted ads. A majority of the FTC Commissioners have indicated their support for a Do Not Track mechanism.

Since the report was issued, the Do Not Track proposal has received a great deal of attention. We've seen some industry initiative in this area—at the major browser companies and within the advertising industry. The international interest in Do Not Track is considerable among our counterpart regulators. And the World Wide Web consortium, an international community whose mandate is to lead the World Wide Web to its full potential through the development of standards, held a workshop on Do Not Track in April.[5]

Our thoughts about Do Not Track have evolved and I'll share some of those thoughts with you. We have identified 5 essential components to a successful Do Not Track mechanism:

- First, Simplicity: If consumers can't find it and figure out how to use it, it's a non-starter.

- Next, Effectiveness: It has to stop all tracking by traditional http cookies, Flash cookies, or whatever else. Do Not Track choices by consumers must be respected. We recently brought a case against a company that offered an opt-out of behavioral targeting that expired after 10 days, a very brief shelf life that consumers did not know about.[6] This company is now subject to an FTC order with a much longer shelf life: 20 years. And perhaps the most important effectiveness measure that we're thinking about in connection with Do Not Track is that there must be a way for it to be enforced.

- Third, Universality: A Do Not Track mechanism needs to be universally honored across companies and industry. Consumers cannot be expected to have to make their choice on a company-by-company basis.

- Fourth, not just advertising. Industry folks sometimes ask me why there would be a problem if information about consumers is collected but not used for advertising. This is still a problem. Some consumers may object not just to targeted advertising but to the data collection in general. This is the kind of data that can be sold to data brokers, insurance companies, or employers. Consumers must be able to opt-out of the actual collection, not just the advertising. I am, however, a reasonable person, and I think the FTC is a reasonable agency. We recognize that certain exceptions would apply for commonly accepted purposes, such as detecting fraud.

---

[4] Fed. Trade Comm'n, *Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Businesses and Policymakers*, at 63-69 (2010) (preliminary FTC staff report).

[5] W3C, "W3C Workshop on Web Tracking and User Privacy April 28-29, 2011, Princeton, NJ" (2011) (agenda, materials) *available at* http://www.w3.org/2011/track-privacy/agenda.html.

[6] *In the Matter of Chitika, Inc.* FTC File No. 1023087, *see press release, available at* http://www.ftc.gov/opa/2011/03/chitika.shtm.

- And last, Persistence: An effective Do Not Track mechanism would ensure that consumers' choices will be persistent. Consumers should not have to reset their preferences every time they clear their cookies or close their browsers.

We asked in the report whether Do Not Track should apply in the mobile context. The answer, at least for me, is "Yes".

But I do recognize that the mobile space is quite different from what we now refer to as the traditional online environment. We're taking about apps that operate differently from websites and it can be more complicated. And that's why it became clear to the agency that it is not enough just for the lawyers to be thinking about these issues. Our technologists are thinking about the issues surrounding Do Not Track in the mobile environment.

I would like to take a moment to address the issue of children in the mobile space, although it's not just children, but teens too. As the mother of two teenage boys, I can assure you, they come with their own unique challenges. And not just in the mobile space.

As with the general population, the issues surrounding mobile devices are rapidly increasing among children and teens. The speed at which young folks have adapted to mobile technology is pretty remarkable. Texting, emailing, social networking. They are doing it all. At the same time. They are amazing multi-taskers.

As you may know, we are in the midst of examining the Children's Online Privacy Protection Rule, an examination that began with a roundtable that took place last June.[7] Among other things, we are examining whether the Rule sufficiently encompasses the mobile activities in which children are engaged. The roundtable remarks and the public comments we received indicate considerable consensus that the statute and the Rule were written broadly enough to encompass most forms of mobile communications without the need for changes. Mobile apps, social networks, etc. – COPPA covers them all.

But, there is less consensus in other areas, like texting. There is some question as to whether these would qualify as "online services." Those are the magic words in the statute. So, that's something we're looking at closely. I know that the CTIA filed a comment in connection with this review, and discussed this very issue.

I appreciate the thoughtfulness with which CTIA has participated in our COPPA review, as well as in our larger rethink regarding privacy, including in the mobile space. Our work is greatly enriched by the participation of knowledgeable industry leaders like you.

With that, again, I'd like to thank you for inviting me today and I'd be happy to answer questions.

---

[7] 16 C.F.R. Part 312; *see also* "FTC Seeks Comment on Children's Online Privacy Protections; Questions Whether Changes to Technology Warrant Changes to Agency Rule" *see press release, available at* http://www.ftc.gov/opa/2010/03/coppa.shtm.