State of the Net West
September 19 and 20, 2012
Commissioner Julie Brill

Thank you so much for that kind introduction.

It is great to be here at State of the Net West. Thank you to Tim Lordan and Eric Goldman for inviting me. I can think of no better place to be right now than California, now that this new season is in full swing. While of course it is always nice to get out of Washington—particularly now—I'm not referring to the election season. No, as every parent in the room knows, we just started the most important season of the year: the "back to school" season.

No more worrying about whether your 8-year-old daughter will like the week long day-camp you've signed her up for. No more fretting about your teen-age son sitting inside on a beautiful summer day playing video games with his friends. Yes, many of us are glad to see our kids back in school, ready—or almost ready—for another year of learning.

We might have bought lunch boxes, crayons, and a new dress—or a laptop—to help them get excited about going back to school. Or we might have written a check for an unspeakable amount for college tuition, while wondering whether, in the end, it might be better for all concerned if our kids decide college isn't for them and they instead strive to become the next Mark Zuckerberg, Bonnie Raitt, or Anthony Davis.

Don't tell my kids I said that.

"Back to School" represents a new year of possibilities, and an opportunity to reinvent ourselves. The 4th grader who makes the bold move to eat on the other side of the lunch room, away from her classmates who picked up a nasty habit of bullying over the summer. The middle-schooler who opts for the chess club this year instead of track, leaving her running pals scratching their heads. And the high-schooler who decides that he absolutely will not go to the same college that his father and grandfather attended. Good luck to him.

But let's face it. "Back to school" is wasted on the young. It's time for us grown-ups to take it back. And in that spirit,

out: privacy, particularly in the mobile space; and Do Not Track. These are the issues I'd like to talk to you about this morning.

Consumers are increasingly turning to mobile devices. Educational apps are teaching kids that "i" goes before "e" most of the time, and that ´ (pi) is an irrational number all of the time. And of course kids—as well as adults—turn to apps for so much more: shopping, engaging with friends on social media, playing games, watching movies—even dating. Fifty-two percent of college students say they often check their phones before getting out of bed, and nearly half do so while in bed at night before falling asleep.[1] Indeed, many of us adults sleep closer to our smartphones than we do to our spouses.

A majority of U.S. mobile subscribers now own smartphones.[2] And the growing dependence on mobile is even more salient in some of our communities. About 40 percent of people in households earning less than $30,000 say they go online mostly through their phones, compared with just 17 percent of those earning more than $50,000.[3] And half of African-American cellphone internet users, and 40% of Latino cellphone internet users, do most of their online browsing on their phones.[4]

As I travel around and speak to companies active in the mobile space, I notice that they too are eager to learn. They are interested in the FTC and our role as the nation's premier consumer protection and privacy agency. As our enforcement actions concerning privacy practices gain more attention, app developers, app service providers and others in this space realize that they need to think more about privacy issues.

Of course, the tech community is well aware of our enforcement actions involving Google and Facebook's privacy practices, including the $22.5 million record-breaking civil penalty that Google will pay for evading Apple's privacy protections for Safari users.[5] Industry players are also well aware that we are requiring both Google and Facebook to develop comprehensive privacy programs that an outside auditor will assess for the next 20 years.

---

[1] Digital News Test Kitchen, *Smartphone Survey Questions & Results*, (2010) *available at* http://testkitchen.colorado.edu/projects/reports/smartphone/smartphone-appendix1/

[2] Nielsen Wire, *America's New Mobile Majority: A Look at Smartphone Owners in the U.S.*, (May 7, 2012) *available at* http://blog.nielsen.com/nielsenwire/?p=31688

[3] 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,*

Our enforcement activity, however, is not limited to the large players. We charged a marketer of children's gaming apps for its failure to comply with the requirements of the Children's Online Privacy Protection Act.[6] And we brought an enforcement action involving a peer-to-peer file sharing app that failed to sufficiently protect the private information of consumers.[7]

When it comes to mobile, many of the players are not household names, and so our enforcement actions have involved companies that may not be on the tip of everyone's tongues. But the lessons learned from these actions are just as important as the lessons learned from our actions against Google and Facebook.

Consumers too are becoming aware of some of the privacy issues involving mobile technologies. With more and more frequency, they read about apps that engage in unknown and unauthorized access to their address books, their photos and videos, their precise location, their every keystroke—raising concerns that their private information is no longer private.

These concerns are heightened when it comes to children. Earlier this year, the FTC took a look at kids apps available in the two largest app stores—Apple and Android. We examined the types of apps offered and their disclosures about data collection.[8]

I'll tell you what we found—or rather—what we didn't find.

App developers and marketers are providing little information about their data practices prior to download. In the apps we studied, it was difficult to determine whether the app collected any data at all, and if it did, what type of data, for what purpose, and who had access to that data.

These troubling findings are not limited to children's apps or to disclosures in the app store. In July, the Future of Privacy Forum found that only 48% of free apps and 32% of paid apps provide access to a privacy policy in the app or through a link within the app.[9] This means
0 0000ma

> 54% of app users have decided to not install a cell phone app when they discovered how much personal information they would need to share in order to use it.
>
> 30% of app users have uninstalled an app that was already on their cell phone because they learned it was collecting personal information that they did not want to share.
>
> Taken together, 57% of all app users have either uninstalled an app over concerns about having to share their personal information, or declined to install an app in the first place for similar reasons.[10]

Improving privacy in the mobile space will not only benefit consumers. Increasing consumer trust also will benefit app developers and marketers, and others operating in this space.

The challenge we face, however, is how to improve mobile privacy practices.

One of the biggest difficulties comes from the number players in the mobile ecosystem, and how diffuse they are, making it tough to keep track of how consumer information is collected, used and shared throughout the ecosystem.

Mobile carriers, device makers, platform developers, app store operators, app developers, ad service providers, and plug in operators all may have access to personal information about consumers.

With so many players, it is perhaps too easy to think that privacy is someone else's responsibility. But that is not the most productive way to think about privacy, as some of our enforcement actions show. A better focus would be for all the companies in the ecosystem to develop a sense of shared responsibility, to ensure that they inform consumers in a realistic and meaningful way about how they collect and use information, so consumers can make knowledgeable choices about how their data is used.

One way to do this is by recognizing the ability of some players in the mobile ecosystem to assist development of appropriate privacy practices by other players.

California Attorney General Kamala Harris has embarked on an effort based on this idea. After the FTC's study about privacy policies—or the lack of them—in the app world came out, General Harris sat down with mobile app platform providers and reached an agreement that begins to address this problem. The agreement requires the platform providers—Amazon, Apple,

---

[10] Pew Internet & American Life Project, *Privacy and Data Management on Mobile Devices*, Pew Research Center (Sep. 5, 2012) *available at* http://pewinternet.org/Reports/2012/Mobile-Privacy.aspx

Google, Hewlett Packard, Microsoft, Research in Motion, and most recently Facebook—to give app developers the means to provide consumers with information about their privacy policies.[11]

One player providing tools to another to increase transparency relating to privacy practices. In a complicated ecosystem, this is the kind of effort that will help app developers and marketers put in place needed privacy protections.

But much more needs to be done. Apps must post privacy policies, but also rise to the challenge of communicating with users in simple terms about their practices. And app developers need to understand the privacy practices of plug-ins and software development kits that collect and use information through their app.

At the FTC, we are working with the mobile community to help it better address privacy issues. We recently published a guide to help app developers adhere to best privacy practices.[12] Early reviewers of our guidance say it is a "must read" for app developers and other companies in this space.

Our guidance encourages app developers to bake privacy into their app from the start. Developers should limit their information collection to the information they need for the proper functioning of their app. And they should ensure the security of the information they do collect. They should collect sensitive information—financial, medical, precise geolocation—only with affirmative consent. They must comply with the provisions of the Children's Online Privacy Protection Act in connection with children's information. And app developers should be transparent about their practices. They should provide choices that are easy to use and understand, and the choices should, of course, be honored.

* * * * * *

Honoring consumer choice is also at the heart of efforts surrounding Do Not Track—a