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, it is during this season that I seek opportunities to look at things with a fresh perspective by educating myself.

And there is no better place for me to do that than here on the West Coast. This is my second extended trip through the Bay Area and Silicon Valley since becoming a Commissioner at the FTC. I cherish coming out here to meet directly with those that are vigorously innovating, driving a great portion of our economy, and surprising and delighting consumers which each new smartphone, tablet and cool app.

Of course, the focus of my educational sojourn here is centered around what this technological revolution means for today's consumers. The Federal Trade Commission is thinking about several issues important to the tech community. But two current hot topics stand

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 π (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,* Pew Research Center (Apr. 13, 2012) *available at* http://pewinternet.org/~/media//Files/Reports/2012/PIP_Digital_differences_041312.pdf.

[4] 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.

[5] Press Release, FTC, Google Will Pay $22.5 Million to Settle FTC Charges it Misrepresented Privacy Assurances to Users of Apple's Safari Internet Browser (Aug. 9, 2012) *available at* http://www.ftc.gov/opa/2012/08/google.shtm

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 that a majority of both free and paid apps do not have easy access to a privacy policy.

Consumers are starting to "vote with their feet"—or their fingertips—and are making choices based on their concerns about the privacy practices of players in the mobile space. They wonder why a flashlight app needs to download their contact list, or why Angry Birds needs their geolocation information. Pew just released a study that showed:

---

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

[7] Press Release, FTC, Peer-to-Peer File-Sharing Software Developer Settles FTC Charges (Oct. 11, 2011) *available at* http://ftc.gov/opa/2011/10/frostwire.shtm

[8] Press Release, FTC, FTC Report Raises Privacy Questions About Mobile Applications for Children (Feb. 16, 2012) *available at* http://ftc.gov/opa/2012/02/mobileapps_kids.shtm

[9] Future of Privacy Forum, *FPF Study Results Show App Developers Heed Call for Privacy Policies* (Jul. 11, 2012) *available at* http://www.futureofprivacy.org/2012/07/11/fpf-study-results-show-app-developers-heed-call-for-privacy-policies/

- 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 mechanism that would enable consumers to make choices about whether they are tracked by third parties online, including in the mobile environment.

Considerable progress has been made on Do Not Track. Microsoft, Mozilla, Apple and most recently Google have indicated they will incorporate Do Not Track choices into their browsers. The Digital Advertising Alliance has developed an icon that appears in its members' ads, providing consumers with a tool to indicate their preferences about behavioral advertising. The DAA has also said it will honor consumer preferences expressed through their browser by the end of this year. All of these developments have been very encouraging.

---

[11] Press Release, State of California Department of Justice: Office of the Attorney General, Attorney General Kamala D. Harris Announces Expansion of California's Consumer Privacy Protections to Social Apps as Facebook Signs Apps Agreement (June 22, 2012) *available at* http://oag.ca.gov/news/press-releases/attorney-general-kamala-d-harris-announces-expansion-california%E2%80%99s-consumer

[12] Press Release, FTC, FTC Publishes Guide to Help Mobile App Developers Observe Truth-in-Advertising, Privacy Principles (Sep. 5, 2012) *available at* http://www.ftc.gov/opa/2012/09/mobileapps.shtm

The various stakeholders also have been working together within the W3C—an Internet standards organization—to develop a standard for Do Not Track, so that there is a common understanding of what all industry players will do when they learn that a consumer prefers to not be tracked.

It has been critical for the W3C process that all stakeholders are at the table—trade groups, individual companies, civil society, academics, and technologists.

The participants have shown tremendous commitment. They've devoted considerable energy and they've been creative. Most importantly, the participants have demonstrated a sincere willingness to compromise throughout the process.

This has enabled the participants to work through a number of thorny issues—and to resolve them. So much progress has been made, and so much hard work has gone into this. Of course, some important issues remain. But it would be a shame if all that progress was wasted by an inability to resolve these remaining issues. That wouldn't benefit anyone. Not industry. And not consumers.

As I know you're aware, a majority of the Federal Trade Commission has called for a Do Not Track mechanism that would not only control the receipt of targeted ads but also allow consumers to prevent the collection of their information. At the same time, the Commission recognizes that there are some necessary and appropriate exceptions to a consumer's ability to prevent this collection.

The participants in the W3C have generally agreed on the necessity for certain appropriate exemptions—like security, fraud prevention, frequency capping, and where the data cannot be linked to a specific user or device. In addition, some stakeholders have called for exceptions for market research and product improvement.

I encourage the W3C participants to carefully define the kinds of activities that should come within the exceptions for product improvement and market research. We need to make sure that these permitted uses are not given such broad meaning that they become exceptions that swallow the rule. On numerous occasions, the FTC and other stakeholders have asked the advertising networks for specific market research and product improvement uses that require retention of linkable consumer data. The advertising networks are the only ones who can make the case for such use; without input from them it will be hard to see how such uses can be justified when a consumer has opted out of tracking.

I look forward to the W3C stakeholders drilling down into this issue.

I also encourage the W3C stakeholders to address appropriate retention periods. In particular, with respect to market research and product improvement, at least as an initial matter, the W3C participants should consider whether, after a short time frame—30 days, for instance — companies should be required to render that data unlinkable and commit not to re-link it, or delete the data altogether.

W3C should address retention periods for two reasons. First, the FTC has always noted the importance of data minimization as a way to enhance data security. Retention periods that appropriately limit the amount of time a company can hold data in linkable form promotes good data security practices. Second, appropriate retention periods will provide consumers with the certainty that their data will not be maintained indefinitely until companies can figure out how to monetize it.

As I said, these are important issues. While it may not be easy to find consensus, failure to reach agreement could be problematic for both industry and consumers. I am concerned that, if consumers are not provided with an agreed-upon universal means to control the collection of their data, they will increasingly turn to other tools to prevent tracking.

These "self-help" tools are likely to be more blunt than what is currently under discussion in W3C—they may not offer consumers the ability to make granular choices about tracking—and this would be less helpful to consumers and to industry. These self-help tools could also contain more restrictive defaults than currently under discussion in W3C.

Without a common standard in place, we could see an increased technological "arms race," with consumers using new tools to block tracking, and trackers trying to circumvent those tools.

We can avoid heading down this less desirable path by harnessing the good work that has been done thus far in W3C, and coming to closure on this important process. Consumers will benefit from a greater understanding of information collection and use practices, and implementation of necessary protections. Business will benefit because they will attract and retain more customers by assuring consumers that the information they want to be private will remain just that—private.

While some may be looking at the clock and waiting for the recess bell, I say, let's sharpen our number 2 pencils and get this done. Now is the time.

And speaking of time, I think it is time to open this up for discussion, so I can hear—and learn—from all of you.

Thanks very much for inviting me here to speak, and for listening.