"Privacy On the Go:
Privacy Protections in the Mobile Environment"
Remarks of Federal Trade Commissioner Julie Brill
DLA Piper Privacy Symposium
March 6, 2013

Thanks very much to DLA Piper and Jim Halpert for inviting me to kick off your symposium today. And I am especially grateful to see all you hardy souls here in spite of the weather. Those of us who hail from heartier environments are certainly enjoying this "snowquester".

Jim gave me the choice of speaking to you today about any topic I wished. And for obvious reasons – or at least reasons that I think you will find obvious – I have chosen to speak about privacy in the mobile space.

Consumers are increasingly turning to mobile to manage many facets of their lives – everything from shopping, listening to music, catching up on news, buying movie tickets, and locating a nearby restaurant, to getting driving directions, and tracking calories and exercise routines. With our smartphones in hand, we can locate our children. We can play games. We can do our banking and pay our bills. Whatever you'd like to do, there's "an app for that."

And let us not forget: with our smartphones, we can even make phone calls!

Indeed, smartphones are not one device – they are multiple devices wrapped into one sleek unit. They are the Swiss Army knife of our modern age: a powerful collection of services and functions in one handy package that slips right into our pocket. If it only had a corkscrew on the side, it would be perfect.

And who knows, even that might come standard on the iPhone 6.

In addition to doing more and more with our mobile smart phones, we know that more and more of us are using them. In 2011, over 550 million smartphones and tablets were shipped worldwide, exceeding shipments of desktop and laptop computers for the first time ever.[1] In fact, industry watchers say that by the end of 2013, the number of internet-connected mobile devices will exceed the number of people on earth.[2] And the number of mobile users around the world will grow by 1 billion over the next five years.[3]

---

[1] *See* Press release, Canalys, Smart phones overtake client PCs in 2011 (Feb. 3, 2011), *available at* www.canalys.com/newsroom/smart-phones-overtake-client-pcs-2011.

[2] CISCO WHITE PAPER, CISCO VISUAL NETWORKING INDEX: FORECASTING AND METHODOLOGY 2011 – 2016 (Feb. 6, 2013), *available at* http://www.cisco.com/en/US/solutions/collateral/ns341/ns525/ns537/ns705/ns827/white_paper_c11-520862.pdf.

[3] *NetworkWorld, "Mobile Data growth accelerating worldwide, led by smartphone users" (Feb. 7, 2013), available at* http://www.networkworld.com/news/2013/020713-cisco-data-report-266499.html.

Here in the U.S., more than one-half (50.4%) of consumers now owns a smartphone,[4] and that number also is expected to grow.

Our 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 mobile phones, compared with just 17 percent of those earning more than $50,000. And half of African-American cellphone internet users, and 40% of Latino cellphone internet users, do most of their online browsing on their phones. And if you have teens, you know they are never without their phones. Nearly half of college students say they often check their phones before falling asleep, and over half do so before getting out of bed in the morning.[5]

Along with the explosion in popularity of our smartphones has come an explosive growth in the potential collection and use of the myriad forms of data generated through our smartphones. Our location as we walk around with our phones in our pockets, our contact lists, our emails, our photos, the books we read, our online searches, our shopping habits, the text messages and phone calls we make and receive, and so much more – it's all potentially available through our smartphones. And there are a large number of players who may have access to this information – platforms and operating systems, app developers, plug ins, ad networks and other third parties that provide features to make users' experiences richer.

Consumers are becoming aware of some of the privacy issues involving mobile technologies. With more and more frequency, consumers 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.

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 recently released a study demonstrating that 57 percent of app users have uninstalled or declined to install an app once they understood how much personal info they would need to share.[6]

Businesses are starting to respond. Just two days ago, the New York Times noted that competition around privacy – where businesses are touting their privacy protective practices – is on the rise. [7] Microsoft's chief privacy officer declared that companies like his have come to appreciate the "market forces at play with privacy."[8]

---

[4] 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.

[5] Mashable, *In a Relationship, College Students and Their Smartphones* (Jan. 30, 2012), *available at* http://mashable.com/2012/06/30/smartphones-college-students-infographic/ .

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

[7] Somini Sengupta, *Web Privacy Becomes a Business Imperative*, N.Y. TIMES, *available at* http://www.nytimes.com/2013/03/04/technology/amid-do-not-track-effort-web-companies-race-to-look-privacy-friendly.html?_r=0.

So improving privacy in the mobile space will not only benefit consumers. Earning consumer trust will increasingly become a market imperative for browsers, websites, app developers, marketers, and others operating in this space, and allow this highly innovative segment of our economy to continue to thrive.

As the nation's premier consumer protection and privacy agency, we at the FTC are committed to translating our long-standing consumer protection principles into the innovative and complex mobile space.

In the "on the go" mobile world, this translates into providing consumers with information "just in time" and through "consumer friendly" layered notices. The FTC's call for providing better consumer choice and transparency, laid out in our big privacy report issued one year ago, applies with even greater urgency in the mobile space – where there is limited real estate, making textual disclosures hard to read, and where consumers now have limited understanding of how much of their information can be collected and used, and by whom. We are working hard to get out the message that all players in this ecosystem have a responsibility to provide more transparency and appropriate choices to consumers.

We have our work cut out for us. We have found that many players in the mobile ecosystem are still not even providing more traditional privacy policies. In 2012, the FTC released two studies that assessed the adequacy of privacy disclosures made in mobile apps directed to children.[9] We found that the majority of kids apps do not adequately give parents the information they need to determine what data is being collected from their children, how it is being shared, or who will have access to it. Probably most troubling is that many of the apps we studied shared certain information with third parties – such as device ID, geolocation, or phone number – without ever disclosing that fact to parents.

As we dive deeper into mobile issues, we have learned that understanding the technology is critical. So we have brought in top-notch computer scientists to advise the agency on evolving technology and to assist us in our enforcement and policy work. Ed Felten of Princeton served as the FTC's first chief technology officer. After Ed returned to Princeton a few months ago, Steve Bellovin of Columbia University took over. Steve is a cyber-security expert who, prior to becoming a professor at Columbia, had spent many years doing highly innovative work at Bell Labs and AT&T Research Labs. We are extremely fortunate to have him. For the techies in the crowd – and even for those of you who, like me, only play techies on TV – I commend Steve's blog to you: tech@ftc.

We also have established a Mobile Technology Unit, where we have dedicated attorneys and technologists who provide assistance and coordination on mobile cases and policy work throughout the agency. And we have created a mobile lab, with various undercover mobile devices and platforms, that are invaluable in our law enforcement efforts.

---

[8] Id.

[9] Mobile Apps for Kids: Current Privacy Disclosures are Disappointing (Feb. 16, 2012), *available at* http://www.ftc.gov/opa/2012/02/mobileapps_kids.shtm ; *and* Mobile Apps for Kids: Disclosures Still Not Making the Grade (Dec. 10, 2012), *available at* http://www.ftc.gov/opa/2012/12/kidsapp.shtm .

These law enforcement efforts have been bearing fruit. Of course, the tech community is well aware of our enforcement actions involving Google and Facebook's privacy practices, including the record-breaking $22.5 million civil penalty that Google paid for evading Apple's privacy protections for Safari users.[10] 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.

Our enforcement activity is not limited to companies that are household names, and these less-well known cases bear similarly important lessons for the tech community. I'm not sure whether you all have noticed, but we are barely nine weeks into 2013, and we have already announced 3 mobile cases.

Our most recent case involved mobile device manufacturer HTC, in which we were concerned that HTC failed to employ reasonable measures in the design and customization of its software on its mobile devices, and so put at risk sensitive information about millions of consumers.[11] We believed that HTC failed to provide its engineering staff with adequate security training, failed to test the software on its devices for security vulnerabilities, and failed to follow well-known and commonly accepted secure coding practices. While these practices raise concerns similar to those we have had in many of our other data security cases, some of you may have noticed that the HTC matter did not involve enterprise security, and instead focused on software vulnerabilities, an interesting development.

Last month we also announced a settlement with Path, a social networking app that allows millions of users to keep journals of "life moments," thoughts, photos, and songs to share with their networks of friends.[12] We believed that Path deceived users by collecting information from their mobile device address books without users' knowledge or consent. We also believed that Path violated the Children's Online Privacy Protection Act (COPPA) by collecting personal information from approximately 3,000 children without getting parental consent.[13]

Our order requires Path to pay $800,000 for violating COPPA, and prohibits the company from collecting information from children without first obtaining permission from parents. The order also requires that Path implement a comprehensive security program, including biennial assessments from a qualified third party auditor for 20 years.

---

[10] *See* Press Release, 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://ftc.gov/opa/2012/08 /google.shtm.; *and See* Press Release, FTC Charges Deceptive Privacy Practices in Google's Rollout of Its Buzz Social Network (Mar. 30, 2011), *available at* http://www.ftc.gov/opa/2011/03/google.shtm.; and *In the Matter of Facebook, Inc., a corporation* FTC File No. 0923184 (2011).

[11] *See* Press Release, HTC America Settles FTC Charges It Failed to Secure Millions of Mobile Devices Shipped to Consumers (Feb. 22, 2013), *available at* http://ftc.gov/opa/2013/02/htc.shtm.

[12] *See* Press Release, Path Social Networking App Settles FTC Charges it Deceived Consumers and Improperly Collected Personal Information from Users' Mobile Address Books (Feb. 1, 2013), *available at* http://www.ftc.gov/opa/2013/02/path.shtm.

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

And a few weeks earlier, we settled with another mobile app company for violations of the Fair Credit Reporting Act.[14] [15] We believed that, despite its disclaimer that it was not a credit reporting agency, the company, known as Filiquarian, did act as a credit reporting agency when it advertised that its mobile apps could be used to access criminal records and conduct searches on potential employees. Our order requires the company to comply with the FCRA, including furnishing consumer reports only to those with a permissible purpose, and providing users with information about their obligations under FCRA.

Our enforcement cases serve an important role in educating the technology community. We know that most companies in the mobile ecosystem want to do the right thing with respect to how they collect and use information, and how they notify consumers about their practices. So in addition to our enforcement efforts, we have been engaged in several policy initiatives that set out best practices with respect to privacy for companies in the mobile space.

One of the biggest difficulties in developing best practices comes from the sheer number players in the mobile ecosystem, making it perhaps too easy for some firms to think that privacy is someone else's responsibility. But that is not the most effective way to think about privacy. 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 collected and used.

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

California Attorney General Kamala Harris has embarked on an effort based on just this idea. After the FTC's study about privacy policies – or the lack of them – in the app world came out, General Harris worked with mobile app platform providers to begin to address this problem. The platform providers – Amazon, Apple, Google, Hewlett Packard, Microsoft, Research in Motion, and most recently Facebook – agreed to give app developers the means to provide consumers with information about their privacy policies.[16]

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 improve privacy protections.

---

[14] *See* Press Release, Marketers of Criminal Background Screening Reports To Settle FTC Charges They Violated Fair Credit Reporting Act (Jan. 10, 2013), *available at* http://www.ftc.gov/opa/2013/01/filiquarian.shtm.

[15] 15 U.S.C. § 1681s(a)(2)(A).

[16] *See* Press Release, State of Cal. Dep't of Justice: Office of the Att'y Gen., Attorney General Kamala D. Harris Secures Global Agreement to Strengthen Privacy Protections for Users of Mobile Applications, (Feb. 22, 2012) *available at* https://oag.ca.gov/news/press-releases/attorney-general-kamala-d-harris-secures-global-agreement-strengthen-privacy.

This perspective of shared responsibility is also the focus of our new mobile privacy report, released last month.[17] The report makes recommendations for "best practices", focusing on how each of the players in the mobile space – platforms, app developers, advertisers, analytic companies, and trade associations – has an important role to play in protecting consumers' privacy. Let me highlight a few of the report's recommendations for best practices.

Platforms and operating systems like Apple, Google, Microsoft and Research in Motion should provide "just in time" disclosures and affirmative express consent before allowing apps to access users' sensitive content, like geolocation information, contacts, photos, and calendars. Platforms should also consider developing a consumer-facing one-stop "dashboard," where consumers could review and manage the types of content accessed by the apps they have downloaded. And implementation of a Do Not Track mechanism by operating systems will provide consumers with an appropriate way to express their preferences about data collection and use that can be conveyed to web-enabled services as well as apps.

Turning to app developers, we recommend that they make their privacy policies accessible through app stores, and provide "just in time" disclosures and affirmative express consent for sensitive information, if the platform doesn't provide such a consent mechanism. And app developers should improve coordination and communication with ad networks and other third parties so app developers can provide accurate disclosures to consumers.

As for ad networks, analytics companies, and other third parties, they should communicate with app developers so that developers can provide truthful disclosures to consumers about data collection and use.

The point is that the complexity of the ecosystem demands that all participants play a role. Many companies – including some app developers, platforms, and trade associations – have already begun to address these issues. I want to applaud their ongoing efforts. But while some companies are doing a good job of following these principles and protecting consumers, others need to step up to the plate. If not, these players may face more proscriptive rules down the road, or they may simply be left in the competitive dust.

Mobile is exciting and feels different. If we can continue to reorient all players throughout the ecosystem to develop privacy and functionality in tandem, then I think we are on our way to creating a trusted environment where consumers feel safe, and where industry can continue to innovate and delight consumers by providing the products and services that consumers want.

Thanks very much.

[17] Mobile Privacy Disclosures: Building Trust Through Transparency *(Feb. 1, 2013), available at* http://www.ftc.gov/opa/2013/02/mobileprivacy.shtm.