"The Perfect Gift"
Keynote Address by Commissioner Julie Brill
Before the Direct Marketing Association
March 12, 2013

Thank you so much for that kind introduction.

And thank all of you for taking time out of your busy conference schedule to join me here to celebrate my birthday.

I'll speak briefly because I am especially anxious to get to the gift-opening portion of the evening and see what you bought for me. I am positive you'll have done better than my husband. He gave me pearl earrings, which looked nice enough—and were certainly an improvement over last year's vacuum cleaner—but he failed to disclose that when he made his purchase online, the word "imitation" preceded the word "pearl."

So clearly we have here a case in which the dot com disclosure was fine, but the spousal disclosure was less than adequate.

Don't worry if you forgot your gift, by the way. I am sure you all have apps on your smartphones that will let you order while I talk. It wouldn't surprise me if some of them are capable of getting your gift delivered here, gift-wrapped, before the end of the evening. And of course you data brokers out there will have no problem figuring out what I want, but for the rest of you, let me give you some advice. Go ask the data brokers.

But in the event you'd rather hear it from me, I'll just tell you.

The gift I would like from all of you tonight is to accept that we share a common goal—a vibrant and innovative online and mobile marketplace fueled by the responsible use of consumer data. And, that we are all committed to working as hard as it takes to get there.

All of you here tonight know the FTC as the nation's leading consumer protection agency. But we are equally focused on keeping markets competitive and vibrant. Our efforts to build a framework to safeguard consumer privacy in an increasingly high tech marketplace falls, I believe, into that category: it is as much pro-business—pro <u>your</u> business—as it is pro-consumer. We don't think these goals are mutually exclusive.

Lately, more and more analysts are coming to a similar conclusion. Just last week, the New York Times ran an article headlined: "Web Privacy Becomes a Business Imperative."[1] The lead paragraph read: "Privacy is no longer just a regulatory headache.

[1] Somini Sengupta, *Web Privacy Becomes a Business Imperative*, N.Y. TIMES, Mar. 3, 2013, *available at* http://www.nytimes.com/2013/03/04/technology/amid-do-not-track-effort-web-companies-race-to-look-privacy-friendly.html?pagewanted=all&_r=0.

Increasingly, Internet companies are pushing each other to prove to consumers that their data is safe and in their control."[2]

Industry has come to recognize that over the last couple of years, consumers have become much more savvy about behavioral advertising, online tracking, and big data. The book *Big Data: A Revolution That Will Transform How We Live, Work and Think* made it into the top 25 best-selling books on Amazon within 24 hours of its release.[3]

And mobile commerce is the newest big data opportunity. As you are all well aware, the FTC has plunged into the ever-expanding sea of the mobile space, both ramping up our enforcement efforts and researching policies that rise to the dual challenge of protecting consumer privacy, while allowing the exciting mobile marketplace to thrive.

And thrive it has. Consumers are increasingly turning to mobile to manage many facets of our lives. With our smartphones in hand, we can locate our children. We can play games. We can do our banking and pay our bills. And, of course, buy birthday gifts….

The smart phone has revolutionized how we shop. And it has transformed how you sell. These little devices are constantly transmitting a stream of rich marketing information to a myriad of players, many sitting here today.

While I believe that many of you collecting and using this data are doing so responsibly, we all know that consumers are starting to worry. That's because they now have a better understanding that their every click, purchase, movement, and interest is being recorded and passed on by their mobile devices.

They want to know why a flashlight app needs to download their contacts, and why Angry Birds is tracking their physical location. When they don't get answers that make sense to them, they vote with their feet—or more accurately, their delete buttons. Pew recently released a study showing that 57 percent of app users have uninstalled or declined to install an app once they understood how much personal information they would need to share.[4]

So let me tell you what the FTC is doing to keep these customers—your customers—from abandoning the mobile space or avoiding the apps that collect the data you need to continue to enhance the consumer's experience in the mobile and online marketplace.

---

[2] Id.

[3] VIKTOR MAYER-SCHONBERGER & KENNETH CUKIER, BIG DATA: A REVOLUTION THAT WILL TRANSFORM HOW WE LIVE, WORK AND THINK, (2013).

[4] 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.

We are going after the players that treat sensitive data sloppily; that collect information from children without their parent's consent; or that engage in deceptive or unfair practices regarding the extent to which they are tracking consumers. These sorts of companies are engaging in violations of privacy that we can all agree are bad for consumers and bad for business. And it is these sorts of companies, not the FTC, that frighten customers, sometimes completely out of the marketplace.

When we go after the bad apples, we send a message: There is a cop on the beat, and we are there to help ensure that consumers can safely enjoy the online and mobile space. Indeed, just this year we have already brought three mobile privacy enforcement actions.

In our most recent case, the mobile device manufacturer HTC America agreed to settle charges that it failed to take reasonable steps to secure the software it developed for its smartphones and tablet computers, placing sensitive information from millions of consumers' mobile devices at risk.[5]

And in another case we announced last month, the operator of the Path social networking mobile app, which allows users to keep and share online journals, settled FTC charges that the app had raided users' address books without permission and collected information about children without parental consent, a violation of the FTC Act, as well as COPPA.[6] Path is on the hook for $800,000 to square that latter charge.

And in January, we brought our first mobile app Fair Credit Reporting Act enforcement action. We charged that Filiquarian, a company that sold background screening reports containing criminal records through mobile apps, operated as a credit reporting agency but failed to comply with the FCRA.[7]

Our recent policy initiatives seek to address some of the newer activity we have seen in the online and mobile space. For instance, our recent revisions to the COPPA rule closed a loophole that allowed plug-ins and other third parties to collect personal information about children on child-directed apps and websites without parental notice

---

[5] *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.

[6] *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.; *and* Federal Trade Commission Act of 1914, 15 U.S.C. §§ 41-58 (1914).; *and* Children's Online Privacy Protection Act of 1998, 15 U.S.C. §§ 6501-6506 (1998).

[7] *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.; *and* 15 U.S.C. § 1681s(a)(2)(A).

and consent.[8] In some cases the revised rule will require the third parties doing the additional collection to comply with COPPA. We also expanded the definition of "personal information" to include additional data, such as geolocation information, as well as mobile UDIDs.

And last month, the FTC released a mobile privacy disclosures report that laid out best practices for the myriad of players in the mobile ecosystem.[9] The report will also be useful to inform the Department of Commerce-led multi-stakeholder effort to come up with a self-regulatory code of conduct. Though we crafted specific recommendations for the different players in the mobile ecosystem, the underlying principles for each are the same: provide consumers with accessible, understandable, and relevant disclosures about how their personal data will be handled, and recognize that providing such disclosures and other privacy protections in the mobile space should be a shared responsibility among all the players.

The importance of proper online and mobile disclosures also drove the agency to issue revised guidance on dot com disclosures—a topic I know is of great interest to you. We published the original guidance in 2000 to help advertisers understand how the FTC would enforce the prohibition on deceptive and unfair practices in the then-new realm of online advertising. But since then, we've seen the mass migration of online commerce to the mobile space—where screens are much smaller—and to social media. Clearly, our original concepts needed a little sprucing up.

So, after almost two years, a public workshop, and three public comment periods, we have a new dot com disclosure guidance that shares a birthday with Mitt Romney, Liza Minnelli, James Taylor, and me.[10]

The main principles of the revised dot com disclosures guidance issued today will not surprise anyone, because they are no different than the principles that underlie our efforts to protect consumer privacy—and market integrity and viability—in the mobile space. Consumer protection laws that apply to commercial activities in traditional media apply equally online, including in the mobile environment. That means that when information is needed to prevent a claim from being deceptive or unfair, the advertiser should, when practical, incorporate relevant limitations and qualifying information into the underlying claim, rather than having a separate disclosure.

---

[8] *See* Press Release, FTC Strengthens Kids' Privacy, Gives Parents Greater Control Over Their Information By Amending Children's Online Privacy Protection Rule (Dec. 19, 2012), *available at* http://www.ftc.gov/opa/2012/12/coppa.shtm.

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

[10] .Com Disclosures: How to Make Effective Disclosures in Digital Advertising (Mar. 12, 2013), *available at* http://ftc.gov/os/2013/03/130312dotcomdisclosures.pdf.

If a separate disclosure is absolutely necessary, it must be clear and conspicuous, often not an easy a task in the mobile space when some ads are no larger than a thumbprint. If a particular platform does not provide an opportunity to make clear and conspicuous disclosures, that platform should not be used to disseminate advertisements that require such disclosures. In other words, if you can't do it right, don't do it at all. (This isn't the first time I'm quoting my mother in a speech.)

Here are some other highlights of the revised dot com disclosures guidance: The placement of disclosures should be as close to the triggering claim as possible. Preferably, advertisements should be designed so that "scrolling" isn't necessary in order to find a disclosure.

We also talk about the desirability of making certain disclosures "unavoidable". Design ads in such as way so that the consumer has no choice but to see the disclosures. And we discuss the circumstances under which disclosures through hyperlinks will work, and circumstances where they may not work.

The key, as always, is the net impression of the ad. The revised guidance notes that if a disclosure is not seen or understood by consumers, it will not change the ad's net impression, and won't prevent the ad from being misleading. If an advertiser knows that a significant proportion of consumers are not noticing or understanding a disclosure that is necessary to prevent an ad from being deceptive, the advertiser should remedy that.

Our revised dot com disclosure guidance is a good read. I recommend it to all of you. I think you'll see it as I do: an essential element in our shared goal of inspiring consumer confidence in the online and mobile marketplace.

There are two other areas where we can work together to inspire greater consumer trust and confidence in the online and mobile market place: Do Not Track and increased transparency for data brokers.

Many of you know that I believe Do Not Track has the potential to offer consumers meaningful choices about how their data is collected and used. And a Do Not Track standard enabled by browsers—whether developed through the W3C or elsewhere—would be the most effective way to provide consumers with granular choices that will be honored across platforms—both online and in the mobile space.

I urge all stakeholders to continue their efforts to arrive at a robust, consensus-based Do Not Track standard to allow consumers to make effective choices about tracking.

Data brokers have been in the big data business long before the term "big data" was coined. Today, these highly sophisticated companies know a lot about consumers, but consumers know nothing about them. But, as I alluded to earlier, that is changing. The FTC is in the process of examining data brokers' practices. We've sent out requests for information to nine data brokers and we will be analyzing the information submitted

to better understand industry practices with a view towards issuing a report later this year.[11]

In the meantime, it is important that we focus on ways to increase transparency in this industry. There are data brokers that provide data for marketing to consumers. And there are those that provide information for non-marketing purposes that fall outside the FCRA. However, sometimes these activities can impact eligibility determinations. One area of growing concern is discriminatory marketing offers—qualifying some consumers to be eligible for discounts or other benefits, based on behavioral data, and disqualifying others, all without giving consumers the opportunity to ensure that the information on which these decisions are based is accurate.

I have been engaged in discussions with industry leaders—many of them here in this room—about creating a web portal that would educate consumers about how data brokers use consumer information for marketing purposes. This web portal could also allow consumers to opt-out of having their information used for marketing purposes, particularly if the data broker already provides such an opt-out. And data brokers that provide information about consumers for eligibility decisions should ensure that their dossiers are accurate by allowing consumers to access and correct their information.

These tools—Do Not Track and a web portal to increase transparency of data brokers—are not required as a matter of federal law. But creating these tools to provide greater transparency and increase consumer confidence would be smart business practice.

The biggest threat to today's expanding and innovative cyber-economy is not the FTC. It is not Capitol Hill—which you'll be visiting tomorrow—or academics, or privacy advocates.

Today's biggest threat is the customer made increasingly skittish as she learns how her personal information is collected, used, bought, and sold. We at the FTC and you in the marketing world share a common purpose: making the online and mobile marketplace a safe place for consumers and their families to shop, share, view, and communicate.

This shared goal should enable us all to look at data-driven marketing with the same eye—an eye towards continuing its effectiveness while protecting consumers.

An online and mobile space with respected and secure consumers would be the best birthday present of all.

Real pearl earrings can wait until next year.

Thank you.

---

[11] *See* Press Release, FTC to Study Data Broker Industry's Collection and Use of Consumer Data (Dec. 18, 2012), *available at* http://www.ftc.gov/opa/2012/12/databrokers.shtm.