ANA Advertising Law and Public Policy Conference
Keynote Address by FTC Commissioner Julie Brill
March 29, 2012

Good afternoon and thank you.

We all know what everyone was talking about on Monday morning. We've waited over 15 months for the latest installment. We can't get enough of that inside look at the world of advertising. And when we finally got to see it, it didn't disappoint: drama, new revelations, and sex.

Of course, you know I am talking about the release of the FTC's final report on privacy – and before you go diving through your copy, I made up the part about "sex".

Oh that the FTC's privacy report could have drawn the same attention that Mad Men and Don Draper's return to Sunday nights did! Conversations at the water cooler about privacy by design along with the hums of "Zou Bisou Bisou".

Yet I imagine that a few of you were paying as close attention to the release of our privacy report as you were to the return of Don Draper.

The report was a culmination of a multi-year effort aimed at ensuring that we will continue to live in a world where we have a vibrant and innovative Internet, with loads of interesting and free content, and also a world where consumers trust the online and mobile market to protect their information.

Our agency has long safeguarded consumers' right to privacy, what the intellectual father of the FTC, Louis Brandeis, called "the right to be let alone --the most comprehensive of rights and the right most valued by civilized men." And we are also committed to the thriving Internet marketplace that is one of the keystones to our recovering economy.

In 2010, the FTC issued a preliminary report on privacy in the 21st century. We outlined a series of best privacy practices through which companies can succeed in cyberspace while treating their customers' information with respect and care.

On Monday, we issued the Commission report with the final framework that reaffirms and refines our original work.[1] We put forward three principles that companies should follow when handling personal data: incorporate privacy protections into products as they are developed – that is, privacy by design; simplify the choices that consumers make about how their data is collected and used; and be more transparent by providing better information to consumers about how their personal information is being handled.

Our final report reaffirms our call for a robust Do Not Track mechanism. And we discuss the good work that industry has undertaken over the past year to answer our call. Leading

[1] Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers, An FTC Report (Mar. 26, 2012) *available at* http://www.ftc.gov/os/2012/03/120326privacyreport.pdf.

browser vendors – Microsoft, Mozilla and Apple – now offer browsers that permit consumers to instruct members of the advertising and data collection ecosystem not to track their activities across websites. Mozilla has also introduced a mobile browser for Android devices that enables Do Not Track.[2] And just today Yahoo! has announced that it will provide a header-based mechanism across its platform.[3]

The Digital Advertising Alliance's About Ads icon program is now more fully developed, serving more than 900 billion impressions each month. Advertisers, ad networks and publishers that represent nearly 90 percent of the online behavioral advertising market have now committed to follow the DAA's Do Not Track self-regulatory principles.

The W3C – an international standard setting body – is developing a technical standard for Do Not Track, with the participation of technologists, academics, industry – including some DAA member companies – and consumer groups. The W3C has published two working drafts of its standard – one for desktop and one for mobile – with the goal of reaching consensus in the coming months.[4]

And just last month at the White House, the DAA committed to honor the choices about tracking that consumers make through settings on their web browsers.[5]

So let's recognize the good work that industry has done so far. But let's also recognize that there is more work to do.

The DAA's AboutAds program needs to be both more persistent and easier to use. The DAA does not yet offer a mechanism that would enable consumers' opt-outs to continue after users clear their cookies. DAA's Do Not Track works only partially on Apple's browser and mobile devices. And the interface consumers encounter when they click the DAA icon should become more user-friendly.

Also, I have long been concerned — as some of you know — about the collection and use of consumers' data for certain purposes, like credit eligibility and employment. I was pleased to see that the DAA recently adopted principles that would prevent such collection and use of consumers' information. Now we need to see those principles implemented.

---

[2] *Do Not Track Adoption in Firefox Mobile is 3x Higher than Desktop*, Mozilla Privacy Blog, (Nov. 2, 2011), http://blog.mozilla.com/privacy/2011/11/02/do-not-track-adoption-in-firefox-mobile-is-3x-higher-than-desktop/.

[3] Peter Sayer, *Yahoo Says It Will Implement Do-not-Track Worldwide Later This Year*, PC World, (Mar 29, 2012), http://www.pcworld.com/businesscenter/article/252832/yahoo_says_it_will_implement_donottrack_worldwide_later_this_year.html.

[4] *See* Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers, An FTC Report (Mar. 26, 2012) pages 54-55.

[5] Press Release, Digital Advertising Alliance, White House, DOC and FTC Commend DAA's Self-Regulatory Program to Protect Consumer Online Privacy (Feb. 23, 2012) *available at* http://www.aboutads.info/resource/download/DAA%20White%20House%20Event.pdf.

I think most Americans are not deeply troubled when they receive ads targeted to their interests – though I would appreciate it you and your clients would stop sending me so many "erase those wrinkles now" ads.

Rather, it is the underlying data collection and use that concerns most consumers. In a recent Pew Research Center study, 68 percent of Internet users reported they are "not okay" with targeted advertising "*because* I don't like having my online behavior tracked and analyzed."[6]

Target learned this lesson when they used shoppers' buying habits to predict if a shopper was pregnant, and then sent coupons for newborn items to the moms-to-be. Consumers responded the same way most women do when strangers comment on their pregnancy: with a nasty look and a firm "buzz off." Target ended up having to change their campaign to make it less obvious they knew when women's labor pains would begin.[7]

But there is more to this than the "creepiness" factor, as some describe it, of having all sorts of market analysts and data brokers pouring over the records of purchasing and online browsing habits, as well as our geolocation information and other information gleaned from our computers and smartphones.

I believe that consumers are worried – and should be – about the masses of data that are collected about them, and then packaged, parsed, sold, and resold by largely faceless data brokers. This practice runs afoul of the FTC's recommendation that companies practice data minimization – a key tenet of privacy by design, which is in turn a key principle we believe companies should adopt to protect their customer's privacy.

On the most basic level, collecting and retaining vast amounts of consumer information vastly increases the damage a data breach can cause. But the ways in which that data can be used are just as disturbing, maybe even more so.

Researchers have demonstrated how easy it is to associate the reams of data collected with specific consumers, even when that data had been "deidentified." As Alex Madrigal said in a recent article in the Atlantic, "Right now, a huge chunk of what you've ever looked at on the Internet is sitting in databases all across the world. The line separating all that it might say about you, good or bad, is as thin as the letters of your name."[8]

Mad Men's Don Draper said: "People tell you who they are, but we ignore it – because we want them to be who we want them to be." Some may believe that today it is the opposite – that today, data brokers and others obtain so much information from so many sources that they can precisely – and correctly – profile each of us. But I am deeply troubled by the strong possibility that we are not that far from Don Draper's world, because information brokers and

---

[6] Pew Internet & American Life Project, *Search Engine Use 2012*, Pew Research Center (Mar. 9, 2012) *available at* http://www.pewinternet.org/Reports/2012/Search-Engine-Use-2012.aspx?src=prc-headline.

[7] Charles Duhigg, *How Companies Learn Your Secrets*, N.Y. Times, Feb 19, 2012, *available at* http://www.nytimes.com/2012/02/19/magazine/shopping-habits.html?pagewanted=all.

[8] Alexis Madrigal, *I'm Being Followed: How Google – and 104 Other Companies – Are Tracking Me on the Web*, The Atlantic (Feb. 29, 2012) *available at* http://www.theatlantic.com/technology/archive/2012/02/im-being-followed-how-google-151-and-104-other-companies-151-are-tracking-me-on-the-web/253758/.

others can misconstrue the information or use it in inappropriate ways. And in turn, that can have a real – and negative – impact on people's lives.

A devoted son researches diabetes care options for his ailing mother, and his health insurer may see a reason to raise his premiums. A church volunteer prints out the rules of black jack for a casino night fundraiser, and her mortgage lender may see a gambling problem and a credit risk. A high school senior checks out sites offering synthetic marijuana for a health class report, and the Rotary Club scholarship committee may see a kid with a potential drug problem who will not succeed in college.

The FTC's final privacy report suggests some ways we can address these issues. First, as I mentioned, industry needs to take the further steps we recommend to turn its current "Do Not Target" system into a true "Do Not Track," allowing consumers to specify whether they want business to collect only the data that is necessary for their transactions—such as information needed to ship their purchases or prevent fraud, or to fulfill legal obligations.

Second, it is time to shine a light on data brokers who know an enormous amount about consumers – and profit from that knowledge – while consumers know almost nothing about the data brokers. Data brokers may sell lists to advertisers and other marketers, but they could just as well be providing background information to potential employers, and to those that offer credit and insurance coverage.

The point is, we just don't know, and we should. So I have called for a one-stop shop – a web site – where consumers can find out who is collecting information about them; opt out if they don't want to be marketed to, or correct it if it is going out to someone making decisions about them that can have a significant impact on their lives, like credit, employment, or insurance. The Commission as a whole is suggesting that data brokers work towards providing this kind of transparency to consumers. The data broker industry needs to follow the lead of the ad networks and advertising industry, and step up to the plate develop mechanisms to provide consumers with transparency and some control. In the absence of effective movement by industry to solve some of these problems, I think Congress will take a hard look at this area.

At the FTC we are also thinking hard about how our recommendations should be operationalized in mobile space. While "going mobile" has made so much of consumers' lives easier and quicker, it has made protecting consumer privacy more difficult and complex. Mobile devices are exactly that—mobile – and that means portable – and that means small. Privacy disclosures in the traditional online environment are challenging enough – legalese worthy of the Code of Hammurabi appearing on more screens than the Hunger Games. Try to stuff that into your standard mobile phone, and you have to review tiny screen after screen of disclosures that I challenge anyone to click through without developing severe carpal tunnel syndrome.

The FTC will focus on how industry can provide meaningful disclosures in both the mobile space as well as the traditional online environment at a workshop we will hold on May 30th.[9]

[9] *See* Press Release, FTC, FTC Will Host Public Workshop to Explore Advertising Disclosures in Online and Mobile Media on May 30, 2012 (Feb. 29, 2012), *available at* http://www.ftc.gov/opa/2012/02/dotcom.shtm.

Leaving privacy for a moment, let me talk about the Commission's concerns regarding the Internet Corporation for Assigned Names and Numbers, or ICANN, and its plans to increase dramatically the number of generic top-level domains. For those of you not fluent in geek, top level domains are what comes after the dot in a web address, such as "dot-com" or "dot-org."

At the FTC, we are deeply concerned that scammers will use the planned profusion of new web addresses to confuse consumers into thinking they are dealing with a reputable business. And we know that reputable businesses like the ones represented here today are worried about that too.

I recently attended the ICANN meeting in Costa Rica where I had the opportunity to discuss our concerns about this planned roll out with many of the stakeholders in the ICANN process.

I also had the chance to voice the Commission's concern – one that is shared by the FBI, the US Department of Justice, and other law enforcement agencies – about the impact that a large expansion of top level domain names will have on the accuracy of website registration information.

Website registration information is contained in a database called "WhoIs". This database, currently run by ICANN, has considerable limitations. Adding thousands of new names to the system – with no plans to significantly increase ICANN's compliance staff – will leave those of us in law enforcement unable to track down criminals and fraudsters hiding behind the new gTLDs.

The FTC has called on ICANN to increase its compliance staff, improve the accuracy of Whois data, and most importantly, to go slow on the expansion of gTLDs until we can be sure the expansion won't hinder law enforcement, won't place consumers at risk, and won't penalize legitimate businesses and nonprofits that have an online presence.

***

Our final privacy report and our concerns about ICANN's expansion of top level domains share a theme, one that is central to many of the Federal Trade Commission's efforts: we strive to keep the markets – here, the Internet market, fueled by online advertising – thriving; and we strive to protect consumers – your customers – in that market so they continue to trust, participate, and buy online.

Let me end now, and take a few of your questions. I'll save my rendition of "Zou Bisou Bisou" for next year.

Thank you.