United States Federal Trade Commission
"Privacy: From the Woods to the Weeds"
An Address before the International Association of Privacy Professionals
Privacy Academy
September 15, 2011

Good morning. It's great to be here. Thank you to Bojana for that kind introduction. And thanks to Trevor and the IAPP for inviting me here today.

It is great to be here in Dallas. I am going to begin my remarks today by chatting about one of my heroes – and a hero to many who care about privacy – Louis Brandeis. First, I can't help but note that the hero I think most people are grateful for in Dallas this week is the person who invented air conditioning. And the folks with their finger on the dial at this hotel were obviously trying to welcome me. Back where I come from, Northern New England, it is usually snowing by now! So I feel right at home!

We all know Louis Brandeis is one of the most influential Justices on the Supreme Court. But fewer of you may know that he was also the person who conceived the Federal Trade Commission. At the beginning of the 20th century, Louis Brandeis led a crusade against the large steel trusts and other monopolies that were engulfing this country's economic system. His call to cut back on the economic power of the trusts became the focus of the presidential election 100 years ago.

After Woodrow Wilson won the 1912 election, he asked Brandeis to recommend specifically how to solve the problem of the trusts. Brandeis conceived the Federal Trade Commission, which, at Brandeis's urging, Congress empowered to investigate and prohibit unfair methods of competition with a "broad and flexible mandate, wide-ranging powers, and the ability, at its best, to respond to the needs of changing times".[1]

I am privileged to now serve as one of the Commissioners running the FTC. Our mandate is indeed remarkably broad: to protect the nation's consumers, making sure they are not cheated or misled in the marketplace; and to protect competition, making sure that the marketplace is offering up a wide range of goods and services at the fairest price.

The FTC is the leading federal agency on privacy. Through our law enforcement and policy work, we grapple with how technological advances affect our nation's concept of privacy and data security, and how we can best give consumers knowledge, control and choice about how their personal information is collected and used. And since the Federal Trade Commission is the brainchild of Louis Brandeis, it is fitting that we play this leading role, as Brandeis was one of our nation's leading thinkers about privacy. Interestingly, Brandeis's efforts to forge modern privacy law centered on his concerns about significant technologies that were new in his day.

[1] Winerman, Marc. "The Origins of the FTC: Concentration, Cooperation, Control, and Competition", 71 Antitrust Law Journal (2003), 5-6.

His famous law review article, "The Right to Privacy" successfully advocated for the creation of a tort for breach of privacy. Its focal point was the then-revolutionary phenomenon of "snapshot photography" with light, mobile cameras, which allowed the press to, in his words, "overstep[ ] in every direction the obvious bounds of propriety and of decency"[2]. And in *Olmstead v United States*, where Brandeis issued his famous and influential dissent, arguing that "against the government," Americans have "the right to be let alone,"[3] Brandeis was grappling with the appropriate boundaries for the use of nascent wiretap technology.

The Internet revolution makes snapshot photography and wiretap technology look like child's play. Because of innovations in the Internet, social media, mobile communications, and location-based apps, we can now become friends with people whose voices we've never heard. We can tweet our thoughts to a cyber café full of anyone who wants to listen. We shop for groceries online –share photo albums online – pay traffic tickets online – even date online. Health care workers deliver prenatal care in the farthest corners of the developing world using mobile phones. And populist movements, armed only with Twitter and the Internet, bring down dictatorships.

But all this cyber-wonder does not come for free. Just as technology is extending our reach to the limits of our imagination, many of those providing us with all of these advances are reaching back – harvesting and trading in information about us. The amount of tracking of an individual's behavior online—what sites she visits, what ads she clicks on, what she says when she chats, and where she wanders through the day as she carries a cell phone in her pocket—is unprecedented. It is also largely undetected by the consumer, raising serious privacy concerns.

Granted, much of this data is collected to fuel targeted advertising, a practice that has solved the problem posed over a century ago by one of Brandeis's contemporaries, the great merchant and philanthropist John Wanamaker, who said "Half the money I spend on advertising is wasted; the trouble is I don't know which half." Companies are willing to pay significantly more for targeted advertising, so it is paying for much of the online free content we all enjoy.

If all the data collected online were just to sell movie tickets or shoes, I wouldn't be as concerned as I am. Indeed, many consumers prefer to see ads they are interested in, rather than random ads for products and services they would never purchase. But, I am very concerned about some other uses of data. Like lists of elderly patients who suffer from Alzheimer's disease and similar maladies that data brokers market as "perfect prospects for holistic remedies, financial services, subscriptions and insurance." [4]

And social network chats and online search histories that some firms "scratch and sniff" to provide information to a future potential employer, unbeknownst to consumers. And information about a consumer's history in articles on reducing credit card debt that may be provided to a bank where she is asking for a loan. And information about a consumer's online purchases, including that deep fat fryer, that a health insurance company uses to set its rates.

---

[2] Samuel Warren and Louis Brandeis, *The Right to Privacy*, 4 Harvard Law Review 193, 196 (1890).

[3] *Olmstead v United States*, 277 U.S. 438, 478 (1928).

[4] Karen Blumenthal, *How Banks, Marketers Aid Scams*, The Wall Street Journal, July 15, 2009.

This sort of use of consumers' data is not conjecture. The Wall Street Journal reported last year on one life insurer who developed a way to use information about consumers' consumption patterns to make decisions about their life expectancy, and hence rates and coverage.[5] Other larger insurers are also interested in using this technology.[6]

Furthermore, the sheer volume and vulnerability of personal data collected, traded, and stored has created significant problems. Data breaches are rampant. In the past few months alone, we saw the online marketing company Epsilon expose the email addresses of millions of customers of the nation's largest firms, including JP Morgan Chase, Citibank, Target, and Walgreens. We learned that Google and Apple used our smartphones to collect and retain detailed information about our daily movements. And many consumers panicked when Sony's PlayStation online network was hacked, resulting in the exposure of the personal information of about 77 million gamers worldwide.

The FTC has spent considerable time thinking about how we can formulate a better privacy framework that will allow industry to thrive and will foster more information, while at the same time, addressing some of these more troubling issues, and providing consumers with greater knowledge, control and choice over what happens with their information.

In the December 2010 report on privacy, the FTC staff outlines three critical concepts that guide our thinking on how to improve our privacy framework.

First, we call for companies to build privacy and security protections into new products, not just retrofit them after problems arise. When designing new products and services, the level of security and privacy protection should be proportionate to the sensitivity of the data used. And companies should limit the amount of information collected to what is needed, and retain the data only as long as needed.

Second, we call for companies to provide simpler and more streamlined choices to consumers. One way to do that is to provide "just in time" information to consumers. An additional way is to remove the clutter by exempting "commonly accepted" practices from the first layers of the "just in time" notices There is probably a group of practices that we can all agree are "commonly accepted" – such as sharing data with the shipping company that will deliver the product that you just ordered. By removing disclosures relating to these commonly accepted practices, consumers can focus their attention on more unexpected uses of data.

And third, we call for greater transparency around data collection, use and retention. Consumers should know what kind of data companies collect, and should have access to it again in proportion to the sensitivity and intended use of the data.

---

[5] Leslie Scism, Mark Maremont, *Insurers Test Data Profiles to Identify Risky Clients,* The Wall Street Journal November 19, 2010.

[6] Id.

When taken as a whole, I believe the framework we have proposed is flexible enough to allow businesses and consumers to continue to profit from an innovating, growing, and rich information marketplace, and also sturdy enough to provide guideposts on how to innovate and grow in a responsible manner.

Now we are engaged in the very tough work of moving from the forest to the trees, and even down into the weeds, to get the details right. We have received over 400 comments on our report. We are working our way through them, and continuing our conversations with industry and consumer groups, and other policy makers to develop final recommendations.

One area where the details are critically important is in Do Not Track. A majority of the Commissioners – myself included – has called for development – whether by industry or otherwise – of Do Not Track mechanisms. Mechanisms that will give consumers information about online data collection and use practices, and allow them to make certain choices in connection with those practices. We have identified five necessary elements that we will be looking for in any Do Not Track solution:

First, any Do Not Track system should be implemented universally, so that consumers do not have to repeatedly opt out of tracking on different sites.

Second, the choice mechanism should be easy to find, easy to understand, and easy to use.

Third, any choices offered should be persistent and should not be deleted if, for example, consumers clear their cookies or update their browsers.

Fourth, a Do Not Track system should be comprehensive, effective, and enforceable.

Finally, an effective Do Not Track system would go beyond simply providing an opt out from receiving targeted advertisements. It should allow consumers to opt out from collection of behavioral data for all purposes other than commonly accepted practices.

Industry seems to have heard our message loud and clear. We've seen considerable progress in the development of Do Not Track mechanisms. And we've seen considerable progress in industry's willingness and interest in engaging with the Federal Trade Commission on these issues.

I personally have met with some of those involved in the development of these mechanisms, both from the Digital Advertising Alliance AboutAds program, and from the browser companies. There has been meaningful dialogue and I look forward to continuing the conversation.

And indeed, the Commission is closely watching industry and the various mechanisms and programs that they are developing.

So let's drill down a bit into some of the five necessary elements for any DNT mechanism that I've just described. Let's talk about the details that we at the FTC will be paying attention to in the coming weeks and months, as these programs continue to unfold.

First, we all need to speak the same language. DNT mechanisms enable consumers to make a choice about being "tracked." Is that word -- "tracked" -- being used consistently? I am not sure that it is. Companies and consumers should have a clear and consistent understanding about what can and cannot be done with information about a consumer who has chosen not to be "tracked". And as I've said, the concept of "tracking" should include collection as well as serving targeted advertising.

We also need to come to an understanding about "commonly accepted practices". As I noted, there are certain practices that we can probably all agree are commonly accepted. But there are other practices that are merely common. Because industry is now commonly engaged in certain practices does not mean they are commonly accepted by consumers. For practices that are not commonly accepted by consumers, notice and meaningful choice should be provided.

Next, we need to be confident in the technology—if a consumer makes a choice, the technology needs to function to honor that choice, without any loopholes. In this new age, code is conduct. To get the conduct right, we have to get the technology right. There should be no technological glitches that stand in the way of effectuating consumers' choices in a meaningful way.

The success of any particular Do Not Track mechanism also hinges on wide adoption by industry, and broad-based understanding by consumers. We need a critical mass of industry players honoring the choices that consumers have made. And we will closely examine whether each of the programs is easy for consumers to find and interact with. As the programs gain market visibility we will be keenly interested in learning about consumers' actual experience with different DNT programs.

Broadly speaking, we have seen development of two different types of DNT mechanisms: browser-based, and icon based. We need to closely examine how the two work together. Effective DNT programs will enable a consumer's choice about DNT to be registered and honored no matter which mechanism the consumer chooses to use to express her choice.

And last, for those Do Not Track programs that are not self-enforcing, we will be looking to see whether the program engages in robust monitoring for compliance.

* * * * * * *

The conversations and the efforts surrounding Do Not Track are important, but this only represents one aspect of the larger privacy framework that the FTC has been reconsidering.

Personal information about consumers is in the hands of so many different types of businesses. How that information is collected and used has our full attention. The flip side – and you can't think about one without the other – is the security of that information. Data

security has been, and continues to be, a critical part of our privacy enforcement program. Think about the many diverse entities that must now comply with FTC orders in the data security area: brick and mortar retailers, online retailers, payroll processors, technology companies, data brokers, pharmaceutical companies, social networking companies, and more. Dealing with these breaches was undoubtedly very expensive for these companies: employees are distracted from their primary mission; legal departments must set up compliance mechanisms affecting the entire organization; engineers must redesign and retrofit old data systems with better security; and everyone in the company must deal with the loss of its good reputation. I'm sure many of you in this room work hard to remind the occupants of your company's C-Suite that the entire organization needs to engage in good data security practices – an investment now that will help avoid these costs in the future.

Another issue that I am very concerned about is the activities of data brokers. These entities do not directly engage with consumers, and are essentially invisible to them. But data brokers control details about consumers that can have a direct impact on their credit and financial well-being. That's why one of the principles in the FTC staff report—transparency—is particularly critical for data brokers. Greater transparency and providing consumers with reasonable access to information collected about them are paramount in the area.

And then there are the new activities by some data brokers that I mentioned earlier: selling information about online behavior, and more, to financial firms, landlords, and employers that use this information to decide whether – and on what terms – to provide products, services, housing, and employment to consumers.

When Congress created the Fair Credit Reporting Act, it created clear guidelines on how personal information can be used for credit, employment, insurance and other services. Congress gave consumers a right to know when their personal information is being used for these purposes, and a right to access and correct it. In one recent case, we required a company to pay $1.8 million to settle charges that it inappropriately used information gathered through its sale of credit reports to create a marketing list of individuals who had sought payday loans, so that other sellers could target these consumers.[7] And in another matter we made clear that an entity that scrapes information from the Internet and social networks to provide pre-employment background screening to employers must comply with the FCRA.[8]

New technology has enabled the collection and sale of these new forms of credit reporting data. Along with the new Consumer Financial Protection Bureau, the Federal Trade Commission will continue to ensure that consumers have the right to know that this information has been collected and used to make important financial decisions about them, and have the right to correct that data when necessary.

---

[7] See *U.S. v. Teletrack, Inc.*, No. 1:11-CV-2060 (N.D. Ga. June 29, 2011), *available at* http://www.ftc.gov/opa/2011/06/teletrack.shtm.

[8] Letter from Fed Trade Comm'n to Renee Jackson, Nixon Peabody LLP regarding Social Intelligence Corporation (May 9, 2011), *available at* http://www.ftc.gov/os/closings/110509socialintelligenceletter.pdf.

* * * * * * *

Consumers have embraced many of the amazing innovations that new technologies have brought us. At the FTC, we want consumers to enjoy the benefits of all that is now possible. It is our job to take the aerial view of the new technological landscape, zoom in and take a close look at the forest, and then get into the weeds to figure out what is growing and what might grow in the future.

And as we continue to dive deep into this fertile ground, we will strive to live up to the legacy of Louis Brandeis, by ensuring that, with each new technological revolution, consumers' interests are adequately protected.

Thanks again for having me today.