Introductory Remarks
Chairman Jon Leibowitz
FTC Privacy Roundtable
(December 7, 2009)

Good morning and welcome, everyone.

I spoke on a panel recently about Louis Brandeis, an intellectual father of the Federal Trade Commission who was also a world-renowned reformer and Supreme Court Justice. In 1890, Brandeis and his partner Samuel Warren authored a seminal Harvard law review article on privacy. They wrote that "numerous mechanical devices threaten to make good the prediction that 'what is whispered in the closet shall be proclaimed from the house-tops.'"[1] His concern was photographs, then finding their way into tabloids. Brandeis's and Warren's work was both enormously influential and prophetic in some ways, and helped to shape American jurisprudence on privacy over the course of the 20th century.

The 1960s, as Americans started to lose faith in government, and the 1970s, with the Nixon abuses of government surveillance powers, together with the advent of the computer age created more ferment around citizens' privacy rights vis-a-vis their government. The Privacy Act and the fair information practice principles – the FIPPS – grew out of that environment.

I'd argue that we're at another watershed moment in privacy, and that the time is ripe for the Commission to build on the February behavioral targeting principles[2] and to take a broader look at privacy writ large. Let me explain why.

One of my advisors is about to buy a home computer with a quad-core chip running at 2.66 Ghz. It costs under $2000. In the early 1990s, a *slower* Cray supercomputer cost about $10 million dollars.

These advances have created extraordinary benefits for consumers but also have tremendous implications for privacy. The computer cost of data collection seems to be approaching zero. Data storage costs are unbelievably low too; the efficiency made possible by cloud computing complements unbelievable advances in chip technology. So companies can store and crunch massive amounts of data relatively cheaply.

These developments have allowed companies to collect and use data about consumers in ways that were never feasible, or even conceivable, before. Behavioral targeting is one of many ways

---

[1] Samuel Warren & Louis D. Brandeis, *The Right to Privacy*, 4 Harvard Law Review 193 (1890).

[2] *See* FTC Staff Revises Online Behavioral Advertising Principles, *available at* www.ftc.gov/opa/2009/02/behavad.shtm.

that companies can use data, to try to tease out which consumers – or IP addresses, or uniquely identified cookies – are more likely to respond to a particular ad. Those who attended last week's workshop on the Future of News know that a number of speakers spoke about the importance of revenue from targeting in funding journalism; there are both benefits to companies and consumers from targeting, such as more relevant advertising, and costs in terms of privacy.

Though his words still reverberate today – maybe more so than when he dissented in Olmstead[3] – these technologies have fundamentally changed the privacy landscape in a way with which Brandeis would have been completely unfamiliar. Consumers have to grapple with this brave new world of information without analogies in their experience, and without a real understanding of the ways their information is handled or transferred.

Take Internet advertising for example: how many consumers – at least the ones outside this room – have ever heard the names of the many ad networks that end up with their information in the process of targeting ads? How many people understand the networks' role and other intermediaries' role in the Internet ecosystem? How many people understand what a cookie is, much less how to distinguish a first party from a third party cookie? If brick and mortar retailers tracked a consumer's meanderings around a store in the same way the consumer is tracked online, how would consumers respond? To ask the question is to answer it.

It is not just consumers who are grappling with privacy, many companies are too. In the Commission's *Sears* case,[4] consumers in a sense opted in – for $10 – to a stunning degree of tracking of their web usage. The thrust of our case was that, while the extent of tracking was described in the EULA, that disclosure wasn't sufficiently clear or prominent given the extent of the information tracked, which included online bank statements, drug prescription records, video rental records, library borrowing histories, and the sender, recipient, subject, and size for web-based e-mails.

So consumers didn't consent with an adequate understanding of the deal they were making.

Nobody argues that the folks at Sears are bad people who wanted to do bad things with the information they gleaned from these consumers. To the contrary, I don't think they even knew exactly what they expected to learn from the data. That just demonstrates, though, that people are still feeling their way around what respecting privacy really means.

People have asked me what we expect to get from this roundtable, and where we're headed. I

---

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

[4] *In the Matter of Sears Holdings Management Corporation*, FTC File No. 082 3099 (final consent order approved Sept. 9, 2009).

can honestly say: we don't know. Our minds are open. We do feel that the approaches we've tried so far – both the notice and choice regime, and later the harm-based approach – haven't worked quite as well as we would like. But it could be that this issue is a lot like Churchill's view of democracy: "it has been said that democracy is the worst form of government except all those other forms that have been tried from time to time."[5]

We all agree that consumers don't read privacy policies – or EULAs, for that matter. And I think most people now acknowledge that you can't focus on traditional notions of PII such as name and address, when particular devices – and even consumers – are so readily identifiable without it.

And everyone believes those issues are complex, as reflected in the charts to be introduced in a few minutes. Of course, Commission staff's thoughtful behavioral advertising principles[6] viewed information in this broader, more holistic way.

Is there a better way to protect privacy? An easier way? A framework that conforms to consumers' reasonable expectations that businesses can understand and apply?

If not a "unified theory" of privacy, are there steps to narrow the areas of confusion and empower consumers? Should we utilize more opt-in? Should we treat special categories of information, such as sensitive health or personal financial, differently? How about vulnerable consumers, such as children? We hope that we'll find out over the course of the next six months, and the experts who've graciously agreed to participate in today's discussions will start us off on the course to answering those questions.

Let me thank the many, many people in the Division of Privacy and Identity Protection who've worked so hard to make today's roundtable possible. I won't list everyone, but let me acknowledge the key staff members - Loretta Garrison, Peder Magee, Katie Harrington-McBride, Katie Ratte, Michelle Rosenthal, Naomi Lefkovitz, Jessica Skretch, and Randy Fixman, as well as assistant director Chris Olsen, Associate Director Maneesha Mithal, and of course, Deputy Director (and former DPIP associate director) Jessica Rich and the eminent and distinguished Jeffrey Rosen for helping us think through these issues. Thank you all for assembling such a stellar, accomplished group. And with that, let's get the ball rolling.

---

[5] Winston Churchill, speech in the House of Commons (Nov. 11, 1947).

[6] *Supra*, n.2.