Remarks by Commissioner Julie Brill
United States Federal Trade Commission

Keynote Address

Proskauer on Privacy
New York, NY

October 19, 2010

Good morning. Thank you for that very kind introduction. I am very pleased to be here today to speak to such an interested and knowledgeable audience about the FTC's privacy work. As you may know, privacy is a topic that I have spent considerable time thinking about and working on throughout my career. I am particularly excited to now be a part of the broad privacy efforts underway at the FTC. As you all know, the Commission has led the way among federal agencies in the realm of privacy.

Today I would like to talk about my views on where we are with privacy, how we got here, and where I think we're headed. Then I'll address a few hot topics in the privacy arena, including the industry's new self-regulatory initiative, and teens and privacy.

Where We Are and How We Got Here

I think we are truly at a turning point with privacy in the U.S. As you are all no doubt aware, there has been an intense dialogue – in Washington and beyond – about the appropriate framework for privacy regulation and self-regulation. Advances in technology have challenged our traditional privacy models and caused many of us to re-evaluate those models. Here at the FTC, we have been actively engaged in this dialogue on many levels – holding public workshops, testifying on proposed legislation, and making policy through our law enforcement actions. Very soon, we will release a report on our "re-think" of the FTC's approach to privacy, which we hope will spur further dialogue. I will speak more about the report in a bit.

But first I'd like to talk about the journey we have made to get to this point in our thinking about privacy. Over the past 15 years, we have gone through two stages of thought about the appropriate framework for privacy regulation. First, starting in the mid-1990's, the FTC and others looked at privacy issues through the lens of the Fair Information Practices – the "FIPs" principles of Notice, Choice, Access and Security. This approach called for businesses to provide consumers with notice and choice about how their personally identifiable information would be used. We thought about privacy policies, privacy practices, and various self-regulatory regimes all through the lens of Fair Information Practices.

During this time frame, the FTC, the states, and many consumer advocates called on Congress to enact the FIPs principles into law. While Congress declined to enact

overarching privacy legislation at that time, it did include some of the FIPs principles in laws that were enacted. Most notably, the Gramm-Leach-Bliley Act incorporated a "Notice and Choice" model for financial institutions: consumers are given a yearly notice that they are presumed to read and understand, and then make an "informed" choice. That choice (usually amounting to taking no action at all) often lasts for a long time.

Then, in the early 2000's, the FTC shifted its privacy framework to a "Harm-based" model. This approach focused on harmful privacy practices that present risks of physical security or economic injury to consumers. The top concerns became data security and data breaches, identity theft, children's privacy, spam, spyware, and the like. The FTC and the states brought numerous law enforcement actions addressing these concerns. New data security enforcement tools were created, and others were enhanced. For example, over the past decade many states enacted breach notification laws, and federal regulators adopted the Safeguards Rule under the GLB Act. Congress passed the Fair and Accurate Credit Transactions Act of 2003, which addressed identity theft in a number of ways, including requiring the FTC to promulgate a "red flags" rule and giving consumers a new right of access to their credit reports for free, on an annual basis, allowing them to monitor their reports for suspicious activity, as well as for accuracy.

But in today's technologically advanced environment, these older privacy protection models simply aren't keeping pace. Today, the rapidly evolving Internet and other electronic technologies create much more sophisticated opportunities for companies to gather, use, and retain consumer information. The potentially far-reaching implications of HTML5 is but the latest news about the growing sophistication of data collection capabilities. Rich ecosystems of data now exist, and richer ones will be created, paving the way for some very sophisticated forms of advertising.

These technological developments pose real challenges for our traditional approaches to privacy. For example, the Notice and Choice model, as it is often deployed today, places too great a burden on consumers. Privacy policies have become complex legal documents designed more to shield companies from liability than to meaningfully inform consumers about information practices. Companies issuing these legalistic notices are not necessarily behaving deceptively or unfairly; rather, they are simply responding to the current design of the Notice and Choice framework. Yet it is just not realistic to expect consumers to read and understand these very complex documents and make choices – often without really understanding all the ways in which their information might be used in the future. And it's just not practical to expect consumers to review, let alone understand, these notices on some of the newer Internet-accessible devices such as mobile phones.

The Harm model of privacy regulation also faces challenges in today's advanced technological environment. With its focus on quantifiable or tangible harms to consumers, the Harm model may not adequately address other, less quantifiable harms that are nonetheless real, such as those that can result from the exposure of sensitive information relating to medical conditions, children, or sexual orientation, to name just a

few obvious examples. Also, at its core, the Harm model is fundamentally reactive. As Dan Solove has pointed out, it addresses and corrects privacy and data security breaches after they have been discovered. Stated another way, the Harm model is not a proactive framework designed to encourage companies to include privacy as part of the fundamental design of how they offer products and services to consumers.

Another problem with both the Notice and Choice model and the Harm model is that they rely on a theoretical distinction between personally identifiable information and non-personally identifiable information. This distinction seems increasingly out of touch with technological advances that allow previously non-identifiable data to be "re-identified."

And speaking from the competition side of the FTC's mission, I believe that our traditional privacy frameworks have not been sufficient to promote competition based on privacy – that is, competition among firms based on how they collect, use, store, and dispose of consumers' information.[1] Since much of our current privacy framework is reactive rather than proactive, we currently do little to foster competition on privacy, and as a result we have in fact seen little competition with respect to privacy in the marketplace. A rethinking of the way we view privacy, and efforts to urge firms to build privacy into their business models – the concept of "privacy by design" – may present firms with a greater opportunity to compete on privacy.

In light of these challenges to our traditional approaches, many observers have called for a re-examination of these models. We at the FTC have answered that call.

Roundtables and Upcoming Report

Over the past year, the Commission has explored – in a very public way – a broad array of privacy issues raised by emerging technology and business practices. Through a series of public roundtables and public comments, we have obtained input from a wide range of stakeholders on existing approaches, developments in the marketplace, and potential new ideas. We are now working to finalize our report on what we have learned and where we think we should go from here.

So, what did we learn? Several key themes have emerged from our public process. For instance,

- the collection and use of consumer information – both online and offline – is ubiquitous, and far more extensive than many consumers know.
- consumers lack the understanding and ability in today's environment to make truly informed choices about the collection and use of their data.

[1] For recent discussions of competition based on privacy, *see* Gray, FTC to Boost Competition in Privacy Protection, Global Competition Review, September 23, 2010; Pamela Jones Harbour and Tara Isa Koslov, Section 2 in a Web 2.0 World: An Expanded Vision of Relevant Product Markets, 76 Antitrust Law Journal 769, Issue 3, 2010.

- even in today's environment of ubiquitous social networking, privacy is important to consumers.
- the collection and use of consumer information provides significant benefits: it provides consumers with personalized advertising and other services, and, importantly, it underwrites so much of the free content available to consumers online.
- and, as I alluded to before, the distinction between PII and non-PII is blurring.

Where do we go from here? Our Report is in the final stages of development, but I expect that it will address several major issues, including the following:

First, "privacy by design." This is the idea of building privacy and security into commercial technologies and information practices from the outset – proactively – as opposed to after the fact. Examples include providing reasonable security for consumer data that is collected, limiting collection and retention to those data that are truly necessary, and implementing reasonable procedures to promote data accuracy. The value here, of course, is that when companies implement good practices on the front end, the heavy burden on consumers to navigate complicated privacy policies and effectuate their choices will be alleviated.

Second, transparency. We're looking at ways to facilitate better consumer understanding of privacy practices by improving transparency about commercial data practices. I for one believe – and many others agree – that we need better privacy notices that are shorter, more comprehensible, and more consistent, so that consumers can understand companies' practices and make useful comparisons.

Third, consumer choice. Our roundtables generated a lot of discussion about ways to streamline privacy notices and choices for consumers so that they can focus on the issues that really matter to them. One view, which I share, is that notices should be focused on "unexpected" uses of consumer data, rather than on uses that consumers reasonably expect, such as giving their address to a shipping company in connection with an online product order. This type of streamlining could benefit both consumers and businesses.

A related issue is when to communicate privacy information to consumers. I am of the view that choices are more meaningful if they are presented in real time – at the moment consumers are providing their data, or at the moment their data is being collected behind the scenes.

And of course, no discussion of consumer choice – at least in the online environment – would be complete without acknowledging the strong interest in some quarters in some type of centralized "Do Not Track" mechanism that would give consumers some control over the extent to which their online behavior is tracked. This is a complicated issue technologically, but one that has generated substantial interest and discussion. I personally would like to see a Do Not Track mechanism developed and implemented.

We will more fully explore these and other issues in our upcoming report, which we anticipate releasing soon. The intent of the report will be to offer a framework for future efforts by industry to develop best practices and improve self-regulation, as well as to provide information for policymakers as they tackle these challenging issues. Of course we'll invite public comments on the report, and I want to encourage all of you to give us your views when the time comes.

Self-Regulatory Initiative

Now, I'd like to spend a couple of minutes talking about the current state of industry self-regulation. The Commission has always supported self-regulation in the privacy area, and we will continue to do so. Given the fact that we do not have comprehensive national privacy legislation in the U.S., self-regulation is an important complement to the work being done by the FTC, other federal agencies, and the states, and there are many companies that are trying to do the right thing.

On the whole, however, I personally have not been satisfied with the industry's efforts to date – particularly in the area of behavioral advertising. Since coming to the FTC, I have called for more robust regulatory mechanisms, including universal icons and placement recommendations designed to alleviate consumer confusion about how they can exercise choice with respect to behavioral advertising. I have also called for more stringent protection for particularly sensitive data, such as information pertaining to medical conditions, children, and sexual orientation. And I am particularly concerned about the future uses of legacy data and the potential secondary uses of tracking data.

As you all know, just last week, a group of the major advertising trade associations announced a self-regulatory program designed to allow consumers to opt out of online behavioral tracking by participating industry members. While we do not have all the details yet, and the consumer interface is not operational, I want to acknowledge this effort as a positive step. I am encouraged to see such a substantial segment of the industry making a real effort to address this issue. Of course, the proof will be in the proverbial pudding. When the program is fully implemented, we will be looking closely at this initiative, to see how well it performs on at least three dimensions.

- First, we will examine the program to see how easy it is for consumers to understand and use. This will be critical, because if consumers don't understand the information and controls provided by the self-regulatory program, or they can't easily utilize it, the program simply won't be effective.
- Second, we will look for a robust enforcement mechanism, which is a key component to any successful self-regulatory program.
- And third, we will look for broad participation. Many major industry groups are on board already, which is a very good thing, but it remains to be seen whether less than full participation could lead to consumer confusion.

Privacy and Teens

Next, I'd like to briefly touch on an issue of particular interest to me, as both a policymaker and a parent – and that is the issue of teens and privacy. Teens are heavy users of many of the new technologies that pose such serious challenges to our traditional approaches to privacy. These include mobile devices and new media applications such as social networking, instant messaging, and others. Teens' use of these technologies has changed the way they learn, socialize, and find entertainment.

In so many ways, their experiences are positive, but at the same time, teens face some unique challenges in the online world. Research shows that teens tend to be more impulsive than adults, and they may not think as clearly about the consequences of what they do.[2] Thus, they may share more information online than they should, which can leave them vulnerable to identity theft, have adverse consequences for employment and college applications, and even open the door to bullies or predators.

So the question, as I see it, is how to best help teens navigate these treacherous waters? This is a difficult issue, and I don't have an answer for you today. But it is an important question that I personally believe both regulators and industry must explore further. I hope our report will begin to raise some of the important questions surrounding teens and privacy.

Conclusion

We are facing some very interesting and challenging times in the world of privacy. Technology will advance at an ever more rapid pace, allowing for ever more robust data collection about consumers. It is therefore urgent that we quickly address the privacy concerns that stem from these technological advances, to ensure that consumers will be protected in this new environment.

Thanks very much for inviting me here today to speak to you.

---

[2] *See, e.g.*, Transcript of Exploring Privacy, A Roundtable Series (Mar. 17, 2010), Panel 3: Addressing Sensitive Information, *available at* htc-01.media.globix.net/COMP008760MOD1/ftc_web/transcripts/031710_sess3.pdf; Chris Hoofnagle, Jennifer King, Su Li, and Joseph Turow, *How Different Are Young Adults from Other Adults When It Comes to Information Privacy Attitudes & Policies?* (April 14, 2010), *available at* ssrn.com/abstract=1589864.