

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 nice 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 vision 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 in 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



few obvious examples. Also, at its core, the Harm model is fundamentally reactive. As Dan Solove has pointed out, it addresses security breaches 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. 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 themes have emerged from our public process. For instance, 004 Tc -.0004 Tw [(process.ee em)8TJ -17I-0 at9r TD .ess.eser8>emd ta s



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 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 unique 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 clearly about the consequences of what they do.<sup>2</sup> Thus, they may share more information online than they should, which can leave them vulnerable to identity theft,