Commissioner Julie Brill
United States Federal Trade Commission
The Big Picture: Comprehensive Data Collection
Opening Remarks
December 6, 2012

Thank you, and good morning. It is great to be here and to see so many familiar faces in the room. And because we are being webcast today, I'd like to also say good morning to all of you folks watching on the web as well.

I am here to kick off this workshop, which is designed to help us dive into issues surrounding comprehensive data collection. But before I do, I must take a minute to thank the FTC staff who have put so much effort into pulling this together. This workshop has been organized by the agency's Division of Privacy and Identity Protection, spearheaded by David Lincicum, who has spent the better part of the past few months sparing no detail for today. So thank you David and DPIP.

What I would like to do this morning is talk a bit about what prompted the agency to hold this workshop – and then mention some of my thoughts about this issue, which I'm hopeful can become part of the discussion today.

Two years ago, in December 2010, the Commission issued a preliminary report proposing a new privacy framework for business and policymakers.[1] Our proposed framework was designed to balance consumers' needs to protect their privacy interests with industry's need to innovate, which in part relies on collection and use of consumers' information.

When we proposed this new framework, we discussed the challenges consumers face in understanding the nature and extent of current commercial data practices, and in exercising available choices.

One of the data collection practices we discussed – among many others – was the capability of Internet Service Providers to engage in deep packet inspection. To date, DPI has been used for purposes such as network management and malware prevention.

Because deep packet inspection could also potentially be used to amass information about consumers' every move online, we requested comments on how to appropriately protect consumers from this potentially intrusive technology. In particular, we posed the question of whether deep packet inspection warranted heightened restrictions or enhanced consent.

[1] *See* A Preliminary FTC Staff Report on Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Businesses and Policymakers (Dec. 1, 2010), *available at* http://www.ftc.gov/os/2010/12/101201privacyreport.pdf.

The agency received a significant amount of input on this issue. Some consumer groups – the Center for Digital Democracy and U.S. PIRG, for instance – urged the Commission to oppose any use of deep packet inspection by network operators. Their view is that the profiling capability of this technology severely threatens consumer privacy.[2] The Center for Democracy and Technology singled out deep packet inspection because ISPs serve as the gateway to the rest of the Internet and thus have the potential to conduct profound and comprehensive surveillance.[3] However, CDT believed that any other technology that could also capture a similarly comprehensive picture of a consumer's activities should be held to the same standard.[4]

Some industry commenters said that deep packet inspection is not the only technology that can track nearly all of users' online activity.[5] For example, we heard from Verizon that cookie based technologies could collect the same – if not more – information than could be captured through deep packet inspection.[6] The Internet Commerce Coalition argued that if deep packet inspection technology collects the same information as a behavioral advertising network, deep packet inspection should not warrant heightened restrictions.[7] And the National Cable and Telecommunications Association believed it would be competitively unfair to hold deep packet inspection to a higher standard.[8]

Indeed, numerous technologies can capture large amounts of information about us online or on mobile devices as we go about our lives. Deep packet inspection, social plug-ins, http cookies, web beacons, browser capabilities, and operating system technologies all collect information about our many online and mobile activities.

After reviewing the many comments that we received on this issue, one thing became clear to us: we need to find out more about <u>how</u> to differentiate the data collection capabilities of different technologies. Or even whether <u>any</u> differentiation is appropriate.

Which brings us to today – we are here to learn more. When the Commission issued the final privacy framework in March 2012, we identified comprehensive data collection as one of the areas that required further study. We committed to holding a workshop before the end of the year, and here we are.

---

[2] *See comment of Center for Digital Democracy and U.S. PIRG*, cmt. # 00338, at 37.

[3] *See comment of Center for Democracy & Technology*, cmt. # 00469, at 14.

[4] *Ibid.*

[5] *See comment of AT&T Inc.*, cmt. # 00420, at 21.

[6] *See comment of Verizon*, cmt. # 00428, at 5.

[7] *See comment of Internet Commerce Coalition*, cmt. # 00447, at 10.

[8] *See comment of National Cable & Telecommunications Association*, cmt. # 00432, at 34.

During today's workshop, there are some questions that I will be thinking about as we listen to the presentations and discussions. Perhaps you will find these questions useful as well, so I offer them to you as food for thought.

First, when we addressed data collection and use practices that warrant choice in our privacy report, we put forth the following guiding principle: choice is not required for collection and use of information that is consistent with the context of the transaction or the company's relationship with the consumer.

Today, as we consider the entities that are engaging in comprehensive data collection, let's consider whether these notions of the context of the transactions and the relationship with the consumer might serve as useful frames for thinking about different forms of comprehensive tracking.

Second, let's consider the transparency of data collection and use practices by entities with whom the consumer has a relationship but – in some cases – with whom consumers generally do not interface. These are entities that "run in the background" of our online and mobile lives. Would extensive data collection and use by such entities be consistent with the context of their transaction with consumers? Under what circumstances?

Some are entities that historically have not been collecting information about our activities online, other than for network management or other similar purposes. If they were to start to do so, how should they communicate this change in practices to consumers?

Third, what should happen in the event consumers have inadequate competitive alternatives to choose whether to use the services provided by these entities, or in the event they are locked into the service in some other way.

Fourth, let's think about whether the different technologies used to collect information about the consumer result in substantively different levels of tracking. As we delve into the technologies that enable comprehensive tracking about consumers, we will talk today about ISPs, operating systems, browsers, and ad networks, as well as some additional players in the data collection ecosystem. Do these technologies fall on a continuum in terms of their current or potential data collection activities? Are there bright lines that might separate some from others?

A couple of other points to consider as we launch into these discussions. We know that comprehensive data collection allows for greater personalization and other benefits. We'll hear more about those important benefits as the day goes on, and we know that there are many contexts in which this greater personalization is desirable. But there may be other contexts in which it does not lead to desirable results. In an interesting article in this past Sunday's New York Times Magazine, Professor Jeffrey Rosen of George Washington University described two distinct profiles he created for himself online – Democratic Jeff and Republican Jeff.[9] Each of

[9] Jeffrey Rosen, Who Do Online Advertisers Think You Are?, N.Y. TIMES, Nov. 30, 2012, http://www.nytimes.com/2012/12/02/magazine/who-do-online-advertisers-think-you-are.html?pagewanted=4&_r=0&emc=eta1

these distinct profiles experienced the online world in a very different way. Rosen noted that, with comprehensive tracking that will soon be ubiquitous – moving from offline to online to mobile to digital TV – we will soon see such granular personalization that each individual's digital experience may essentially become one that is created only for him or her. Is this a good thing or a bad thing? Rosen doesn't answer that question, and I suspect that there would be many different answers from those of you in this room today. More interesting to me is the question when will this begin? Rosen does answer this question. He quotes the founder of one of the leading data aggregators as saying this kind of seamless, multi-faceted tracking will begin "once we figure out the privacy rules."

Moving to more fundamental and concrete harms that fall more directly in the FTC's wheelhouse, many of you have heard me speak before about my concerns regarding ubiquitous data collection and use. I am concerned that the rich profiles being created about consumers can be used to harm them at work and in their financial lives. And I'm equally concerned that consumers are unaware of this data collection and use activity or the companies that engage in it, and so have very little opportunity to exercise any current rights they may have to opt out, access or correct this data. Paul Ohm, a professor at University of Colorado at Boulder – who we are delighted is doing a stint here at the FTC and who will be moderating one of today's sessions – has pointed out that the massive combination of facts that companies can gather through comprehensive tracking can lead to "databases of ruin."[10] Databases that make it hard to conceal aspects about ourselves that we would rather not be brought out into the open, and that can harm us with respect to employment, financial opportunities and our reputations.

So that's it for my "food for thought" to start off the day. Now let's begin. First up is Dan Wallach, associate professor in the Department of Computer Science at Rice University in Houston, Texas. Professor Wallach will talk about the different technologies that are capable of comprehensive tracking, and the type of information each of these technologies is capable of collecting. Professor Wallach also is the associate director of the National Science Foundation's Center for Correct, Usable, Reliable, Auditable and Transparent Elections – more commonly known as ACCURATE. His research involves computer security and has touched on issues include web browsers and servers, peer-to-peer systems, smartphones, and voting machines.

I am delighted to turn it over to Professor Wallach. Thank you.

[10] Paul Ohm, Don't Build a Database of Ruin, HARVARD BUSINESS REVIEW, (Aug. 23, 2012), http://blogs.hbr.org/cs/2012/08/dont_build_a_database_of_ruin.html