Commissioner Julie Brill

12th Annual Loyola Antitrust Colloquium

Institute for Consumer Antitrust StI have always had a focus on issues that I care deeply about, and have thought about for many years. It was a true pleasure to join the Federal Trade Commission two years ago, where we have built a formidable powerhouse that handles the field of data security and privacy issues.

In my view, the FTC has, become the leading privacy enforcement agency in the United States by using with remarkable ingenuity, the tools at its disposal to prosecute an impressive series of enforcement cases. Of course, our enforcement work is primarily designed to address the practices at issue in the specific matter. Yet our privacy cases are also more generally informative about data collection and use practices that are acceptable, and those that cross the line, under Section 5 of the Federal Trade Commission Act creating what some have referred to as a common law of privacy in this country.

Two of the agency's most recent cases are important milestones in this developing common law of privacy enforcement. These cases – against the Internet giants Google and Facebook – not only represent important pillars in US privacy enforcement jurisprudence, but also will play an important role in protecting consumers worldwide. We estimate that together, the two companies have more than one billion users around the world. So it is worthwhile to spend a moment reviewing the details of these two cases, to shed light on the lessons responsible companies should draw from them.

The Federal Trade Commission charged Google with deceiving consumers when it launched its first social network product, Google Buzz. We believed that Google took previously private information—the frequent contacts of Gmail users—and made it public in order to generate and populate Google Buzz, without the users' consent and in contravention of Google's privacy policy. The consent order settling this case requires Google to protect the privacy of consumers who use Gmail as well as Google's many other products and services. Now, if Google changes a product or service in a way that makes consumer information more widely

[1] *See* Christopher Wolf, *Targeted Enforcement and Shared Lawmaking Authority As Catalysts for Data Protection in the United States*, BNA Privacy and Security Law Report, Oct. 25, 2010, (FTC consent decrees have "created a 'common law of consent decrees,' producing a set of data protection rules for businesses to follow") and s*ee* Kenneth A. Bamberger & Deirdre K. Mulligan, *Privacy on the Books and on the Ground*, 63 STAN. L. REV. Vol. 63, January 2011, (discussing how chief privacy officers reported that "state-of-the-art privacy practices" need to reflect both established black letter law, as well as FTC cases and best practices, including FTC enforcement actions and FTC guidance).

comment prior to becoming final. Public scrutiny of our consent orders can be quite extensive: in the cases of the Google and Facebook, we received a combined total of nearly 100 comments about our proposed consent orde

Data lately, this is the phenomenon where collection, culling, dissecting and cataloguing of vast

woman's chances of getting a job or a promotion? Could it affect other important aspects of her life?

This is not far-fetched. We've seen press reports about how life insurers use consumer consumption patterns to predict life expectancy, and they use that information to set the rates and coverage they offer.[8] Social media habits can similarly be analyzed as an indicator of future behavior to determine whether someone might be a trusted employee, or a credit risk.

Information can – and will – be scraped from here, there, and everywhere, and then sold to those who are evaluating consumers for jobs, credit, insurance, housing, and other important benefits.

We need to ensure that industry is aware that the FCRA applies in these situations, so that the appropriate heightened protections are in place.

* * *

The Commission's recently released privacy report, setting out a new privacy framework, is designed to address issues like these.[9] Our final framework is intended to articulate best practices for companies that collect and use consumer data. These best practices can be useful to companies as they operationalize privacy and data security practices within their businesses.

The report also includes the Commission's call on Congress to consider enacting baseline privacy legislation, which will provide businesses with certainty and clear rules of the road, and will enable industry to act decisively as it continues to innovate.

There are three main components to the final framework. First, we call for companies to build privacy and security protections into new products. Rather than placing so much of the burden regarding privacy protection on consumers themselves, the report in essence recognizes that companies are often the least cost avoiders of privacy problems, and seeks to reduce costs by shifting some responsibility for addressing these issues to entities that can address them more efficiently – before products are introduced into the market.

Second, we call for simplified choice for businesses and consumers. Consumers should be given clear and simple choices, and should have the ability to make decisions about their information at a relevant time and context.

Third, we call for greater transparency. Companies should provide more information about how they collect and use the personal information of consumers.

Some have expressed concern that our new framework will advantage well-endowed incumbents over new entrants, and tip the competitive forces in favor of the current crop of large providers. But we know that the reality of adhering to the best practices we have identified is not so simple. In some circumstances, new market entrants actually may have a competitive advantage over existing players because they now have a roadmap—our privacy report—that can

[8] *See* Leslie Scism and Mark Maremont, *Insurers Test Data Profiles to Identify Risky Clients,*

guide them as they create new products and services. Existing market players may find it more expensive and difficult to retrofit some of their existing infrastructure and otherwise operationalize the recommendations in the report. The Commission recognized this competitive dynamic, and allowed for a bit more leeway for existing firms – of whatever size – to retrofit their older systems to conform to the new framework.[10] Indeed, many of our recommendations are designed to be scalable, to take into account the different sizes and data practices of companies in the information ecosystem.

Regarding simplified choice—the second component of the report—we have urged industry to develop a Do Not Track mechanism that would enable consumers to make certain choices with regard to being tracked online. Industry has made considerable progress here:

> by developing browser tools and icon-and-cookie based mechanisms;
> by promising to make these mechanisms interoperable; and
> by working on some technical implementing standards.

Do Not Track has the potential to provide consumers with simple and clear information about online data collection and use practices, and to allow consumers to make choices in connection with those practices.

I know that many in industry are worried that providing consumers with choices like Do Not Track will lead large numbers of consumers to opt out of tracking, which could effectively end the ability of platforms and websites to fund free services to consumers through targeted advertising. But the actual experience with providing choices to consumers indicates that this may not be the case. Google offers its users the ability to refine the types of ads they see through its "Ad Preferences" dashboard, and it also offers its users the ability to opt out of tracking entirely. Consumers seem to appreciate knowing how Google has sized up their interests, and they overwhelmingly exercise more granular choices to adjust the ads they will see, rather than opt out. I hope and believe that we will have a more user-friendly Do Not Track system in place by the end of this year, and that industry participants will come to see that it improves the user experience by engendering greater consumer trust.

Yet as we work with the various stakeholders who are developing an easy to use, persistent and effective Do Not Track system, we recognize that there are important competition issues at stake as well. Large firms operating through multiple brands across various websites may have a different view of our recommendations regarding how to define a "first party" than smaller firms operating through a single brand. And firms with a particular business model may push for permitted uses for tracking information across websites that could give them a leg up on their competitors. As we watch industry's continued development of Do Not Track, we will keep a keen eye on these competitive dynamics.

We will also be active in the coming year with respect to data brokers. Data brokers are largely invisible to consumers. Some offer consumers the right to access and correct information, but consumers have no idea how to find many data brokers. To address these problems, the Commission supports targeted legislation that would provide consumers with

[10] *See* Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers, An FTC Report (Mar. 26, 2012) page 31.

access to information about them held by a data br

It's not just the big players. One small search engine's marketing pitch is that it "does not collect or share personal information."[12] It was voted one of the top 50 websites of 2011 by Time magazine.[13]

This is just the tip of the iceberg. In the near future, I believe we will see even more competition among firms based on the privacy attributes of their products and services.

Thank you.

[12] www.duckduckgo.com

[13] http://www.time.com/time/specials/packages/article/0,28804,2087815_2088176_2088178,00.html