Commissioner Julie Brill
12th Annual Loyola Antitrust Colloquium
Institute for Consumer Antitrust Studies
Loyola University Chicago School of Law

"Privacy, Consumer Protection, and Competition"

April 27, 2012

Good afternoon. I'm delighted to be here today. Thank you, Spencer, for inviting me to the 12th Annual Loyola Antitrust Colloquium.

I have been asked to focus my remarks today on privacy—an issue 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 entire 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.[1]

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).

available to third parties, it must seek affirmative express consent to such a change. And we imported into the Google consent order one of the most effective provisions in our many data security cases. We are requiring Google to develop and maintain a comprehensive privacy program and obtain independent privacy audits every other year for the next 20 years.[2]

In our case against Facebook, the Commission alleged a number of deceptive and unfair practices. These include the 2009 changes made by Facebook so that information users had designated private – such as their "Friends List" or pages that they had "liked"—became public. The complaint also charged that Facebook made inaccurate and misleading disclosures relating to how much information apps operating on the site could access about users. For example, Facebook told users that the apps on its site would only have access to the information those apps "needed to operate." But we allege that apps could view nearly all of the users' information, regardless of whether that information was "needed" for the app's functionality. We also claimed that Facebook made promises that it failed to keep: it told users it would not share information with advertisers, and then it did; and it agreed to make inaccessible the photos and videos of users who had deleted their accounts, and then it did not.

Like the Google order, the Facebook order requires Facebook to obtain users' affirmative express consent before sharing their information in a way that exceeds their privacy settings. An important additional provision, not present in the Google order because the facts didn't lend themselves to addressing this issue: Facebook must ensure that it will stop providing access to information after a user deletes it. But like the Google order, the Facebook order requires Facebook to implement a comprehensive privacy program and obtain outside audits for 20 years.[3]

Now some may argue that the common law developed through the FTC's consent orders like those in the Google and Facebook matters is, at best, a "common law light", since courts do not issue the orders through the traditional adversarial process.[4] I would not disagree with this observation, both as a general matter and especially in the context of novel applications of Section 5's unfair methods of competition prong. I would, however, make two points that may be more salient in the context of our privacy consent orders, which typically employ a more traditional analysis under Section 5's "unfair and deceptive acts and practices" prong. The first point is grounded in the rigors of the legal process employed by the FTC. While the FTC's privacy consent orders are not issued by a court of general jurisdiction, the pre-litigation investigatory phase, as well as the process of obtaining Commission approval of staff's recommended resolution, share some attributes of adversarial proceedings. Both staff and target companies could attest to this fact. And although the discussions between the agency and the company leading up to the settlement are not public, the consent orders are subject to public

---

[2] *Google Inc., a corporation* FTC Docket No. C-4336 (Oct. 24, 2011) (Consent order). *Available at* http://www.ftc.gov/opa/2011/10/buzz.shtm.

[3] *In the Matter of Facebook, Inc., a corporation* FTC File No. 0923184 (2011).

[4] *See* William E. Kovacic and Marc Winerman, *Competition Policy and the Application of Section 5 of the Federal Trade Commission Act,* Antitrust Law Journal, Vol. 76, No. 3, 2010. ("one can have confidence in a theory's power and durability only when it has been tested in adversarial proceedings and endorsed by reviewing courts.")

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 orders, many of them quite substantive. The public comment process is one that I take quite seriously.

The other point I'd make is that, whether we call our privacy consent orders a developing "common law" or "common law light", we know that responsible companies collecting and using consumers' information watch our privacy cases very closely, in order to learn about practices that are acceptable, and perhaps more importantly practices that are not acceptable under Section 5. And this is precisely as it should be: the enforcement work of the nation's premier consumer protection agency should be informative to industry, as well as the courts, especially in an area like privacy where technological advances are rapidly changing.

* * *

As powerful as our privacy enforcement work has been, it is precisely because technology is advancing so rapidly that we are facing some potentially serious gaps in our enforcement arsenal. I have been deeply concerned that we may be unable to appropriately protect consumers if we do not evolve our thinking.

One example is the concept of "personally identifiable information" which in the not too distant past meant name and address linked with other information that we had traditionally thought of as identifying an individual. Researchers have demonstrated, however, that it can be relatively easy for a person with appropriate technical know-how to take some types of data that are stripped of identifying information, and reassociate the data with specific consumers. And a great deal of information that is collected and used in the data ecosystem is now linked not to a specific "name", but instead to a specific smartphone or laptop. Given how closely these devices are now associated with each of us — many of us sleep more closely to our cell phones than we do our spouses! — data that are linked to specific devices through UDIDs, IP addresses, "fingerprinting" and other means are, for all intents and purposes, linked to individuals.

Second, the old model of providing consumers with notice and choice about practices concerning information collection and use simply do not work. Privacy policies have become too legalistic, placing too great a burden on consumers to understand and make decisions about complex notions that are challenging even to experts in the field. And when these policies and choices are presented on a mobile device's small screen, the challenges are that much greater. We have found that many mobile app providers do not even bother trying to communicate their data collection and use practices. In February 2012, the Commission released a report about mobile apps aimed at children.[5] We found that in virtually all cases, neither the app stores nor the app developers provided disclosures that told parents what data apps collect from children, how apps share that data, and with whom.

Third, many of us have been fascinated with the promise of "Big Data", and its potential to provide consumers – indeed, society at large – with important benefits. For those of you who are steeped in upward pricing pressure and diversion ratios, and haven't thought much about Big

[5] *See* Mobile Apps for Kids: Current Privacy Disclosures are Dis*app*ointing (Feb. 16, 2012) *available at:* http://www.ftc.gov/os/2012/02/120216mobile_apps_kids.pdf.

Data lately, this is the phenomenon where collection, culling, dissecting and cataloguing of vast quantities of consumer data, from such sources as social media, online behavior, geolocation data and the like, can discern patterns that are not obvious when examining data on a smaller scale. Some researchers have reported how sophisticated analyses of traffic patterns and congestion can be analyzed for smart routing, which could be used to save commuters time and money. Other researchers are using large-scale analyses of data to predict outbreaks of flu and other diseases, and help identify newborn babies at risk of infection, potentially lowering health care costs and saving lives. Clearly there are enormous potential benefits from the use of Big Data.

Yet I am concerned that our current laws may not be well-equipped to deal with the vast collection of data about consumers, some of which can unintentionally – or even intentionally – include sensitive information, such as information about health, finances and sexual orientation. This kind of information deserves heightened protection, and it is not clear to me that such protection is being provided.

The New York Times recently reported on one retailer, Target, and its efforts to develop, through analysis of various online and offline data points, a "pregnancy prediction" score.[6] Target developed this score because it believed that major life changes, such as a pregnancy, create perfect marketing opportunities: at such times consumers are the most receptive to changing their shopping habits. The score predicted not only whether a consumer was pregnant, but also when her baby was due, so that Target could tailor its offers depending on her stage of pregnancy.

Now let's suppose that Target didn't use any health information in creating its pregnancy prediction score. Let's simply suppose that it used "innocuous" data – such as linkage between a woman's purchase of newborn-size diapers and a pattern of purchasing certain types of lotions and other products 7 months earlier – to determine the kind of purchases and other customer habits that indicate a shopper is pregnant. That is, it used non-sensitive information to create a prediction about health status. The same type of innocuous data could be used to make other predictions of a sensitive nature, like sexual orientation, financial status, and the like.

Concerns about the collection of vast amounts of information about consumers, the accuracy of that information, and the appropriate use of that information are not new to this country. These concerns led to the passage – over 40 years ago – of the Fair Credit Reporting Act in 1970 (FCRA).[7]

But the world is a very different place today, and traditional credit reports are not the only source for information about consumers that can impact their ability to secure benefits and opportunities such as employment, housing, insurance, or credit.

Consider a woman who receives a high "pregnancy predictor" score from a different kind of company, one that not only develops the score but also provides it to others. Could this information be obtained and used by an employer or potential employer? Could it impact a

[6] Charles Duhigg, *How Companies Learn Your Secrets*, N.Y. Times, Feb 19, 2012, *available at* http://www.nytimes.com/2012/02/19/magazine/shopping-habits.html?pagewanted=all.
[7] 15 U.S.C. § 1681s(a)(2)(A).

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,* Wall St. Journal, Nov. 18, 2010, *available at* http://online.wsj.com/article/SB10001424052748704648604575620750998072986.html.

[9] Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers, An FTC Report (Mar. 26, 2012) *available at* http://www.ftc.gov/os/2012/03/120326privacyreport.pdf.

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 broker. In the meantime, I have called on data brokers that sell information for the purpose of evaluating substantial benefits for consumers to create a one-stop shop on the Internet that consumers can use to access their information and, in appropriate circumstances, correct it. Congress required the Big Three credit reporting agencies to create such an Internet portal in 1996, when companies' ability to provide consumers with secure and accurate information over the web was at its infancy. The Internet has grown by leaps and bounds in the past 16 years. The credit reporting industry should create a more inclusive portal so that consumers can more easily access and correct their information held by any credit reporting agency, and have these corrections flow to all other credit reporting agencies in the ecosystem.

Another area of interest, particularly given its impact on competition, will be our focus on large platform providers, such as Internet Service Providers, operating systems, browsers, and social media. These large platform providers have the ability to track virtually all of a consumer's online activities. The Commission recognizes the heightened privacy concerns in connection with such tracking, and we have said that, at a minimum, heightened protection should apply to any entity that tracks virtually all of a consumer's online activities, whether through an ISP, operating system or a browser. We believe the appropriate competitive balance must be struck across all technologies capable of engaging in this behavior. In the coming year we will further explore privacy and competition issues related to the potential comprehensive tracking that could be employed by ISPs, operating systems, social media, mobile browsers and other large platform providers.

* * * *

Today the public is much more aware of privacy concerns, in part because of our work – as well as the work of the Administration through the Department of Commerce's White Paper and other Administration efforts, and the European Commission's initiative to reform its data protection framework.[11] The public's increased awareness has jump started firms' interest in competing on privacy. In the online and mobile worlds, where the collection and use of personal information is critical to so many business models, we are starting to see significant efforts by firms to compete on privacy.

We're seeing companies compete on how well they protect information in the "cloud." We're also seeing competition with regard to companies' overall privacy practices. When Google rolled out its new privacy policy to allow tracking of consumers across different Google products, Microsoft encouraged consumers to switch to Microsoft's more privacy-protective products and services.

[11] White House, *Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy* (Feb. 2012), *available at* http://www.whitehouse.gov/sites/default/files/privacy-final.pdf.

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