INTERVIEW WITH FEDERAL TRADE COMMISSION COMMISSIONER JULIE BRILL

JULIE BRILL AND PAUL OHM*

This interview with Commissioner Julie Brill of the Federal Trade Commission is based on her participation in the Silicon Flatirons Economics of Privacy Event on December 2, 2011. http://www.silicon-flatirons.org/events.php?id=1005.

At that event, Paul Ohm interviewed Commissioner Brill.

Ohm: It's been nearly one year since the FTC staff issued its December 2010 preliminary framework report on privacy.[1] What are some significant privacy developments of the past year?

Brill: It's been an incredibly busy year at the Federal Trade Commission. On the enforcement side, as discussed earlier, the agency settled with both Facebook and Google in connection with their privacy practices.[2] We also finalized a settlement with Twitter.[3] We've also brought some cases relating to behavioral advertising—we allege that the opt-outs being offered by the companies to consumers were not effective.[4]

Another important development is the review of the Children's Online Privacy Protection Rule.[5] In September, we issued our proposed revisions to the Rule and comments are due from stakeholders on

* Julie Brill is the commissioner of the FTC. Prior to becoming commissioner, Brill served as the Senior Deputy Attorney General and Chief of Consumer Protection and Antitrust for the North Carolina Department of Justice. Paul Ohm is an Associate Professor of Law at the University of Colorado and the IT/IP Initiative Director at Silicon Flatirons.

1. FTC, PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE: A PROPOSED FRAMEWORK FOR BUSINESSES AND POLICYMAKERS, PRELIMINARY STAFF REPORT (2010), http://www ftc.gov/os/2010/12/101201privacyreport.pdf.

2. Facebook, Inc., FTC File No. 0923184 (2011) (consent order); Google, Inc., FTC File No. 1023136 (2011) (consent order).

3. Twitter, Inc., FTC File No. 0923093 (2010) (consent order).

4. ScanScout, Inc., FTC File No. 1023185 (2011) (consent order); Chitika, Inc., FTC File No. 1023087 (2011) (consent order); *see* FTC, *FTC Puts an End to Tactics of Online Advertising Company That Deceived Consumers Who Wanted to "Opt Out" from Targeted Ads* (Mar. 14, 2011), http://www ftc.gov/opa/2011/03/chitika.shtm.

5. Children's Online Privacy Protection Act of 1998, 15 U.S.C. §§ 6501-6506 (1998).

December 23, 2011. While the Rule is under review, we continue to bring COPPA cases, most recently against a website that held itself out as the "Facebook and Myspace for Kids." In that case, the operator of that website agreed to settle FTC charges that he collected personal information from approximately 5,600 children without obtaining prior parental consent, in violation of the COPPA Rule.[6]

On the policy front, the agency continues to monitor how industry has responded to the agency's call for Do Not Track mechanisms. We are also closely watching the mobile space where privacy concerns are escalated as a result of the ubiquitous collection and sharing of information, and the challenges of providing clear notices and choices to consumers on such a small screen.

Ohm: What choices will Do Not Track mechanisms provide to consumers?

Brill: That is one of the critical elements that we've been focusing on with Do Not Track. Our view is that Do Not Track mechanisms should not only prevent the receipt of targeted advertising, but should also enable consumers to prevent the collection of certain information about them. That is just one of the critical elements that we would like to see in Do Not Track mechanisms. We'd also like to see Do Not Track be universal—a mechanism that would work on all sites. In addition, it should be easy to use, have staying power even if browsers are updated or cookies deleted, and it should be meaningful. That is, if companies do not honor the choices consumers make through Do Not Track, they will face consequences—no loopholes. Finally, I want to see interoperability between the various Do Not Track mechanisms that are available. There are browser mechanisms offered by Microsoft, Mozilla and Apple, and there is a cookie-based system offered by the Digital Advertising Alliance. I'd like to see these systems work together, so that no matter which mechanism a consumer used to express her choice, she'd have it honored across the ecosystem.

Ohm: We've talked today about the limitations of notice and choice and the extent to which notices really provide consumers with the information they need. Should the FTC be more aggressive in articulating the limitations on notice and choice?

Brill: I don't think we should be taking the position that notice and choice are ineffective completely. They certainly have limits, but I don't think it makes sense to dispense with the concept. That being said, it is time to build more privacy protections "under the hood" and not put quite so much "on the dashboard." In other words, some baseline privacy protections should be built into products and services, while some

6. *See* United States v. Godwin, No. 1:11-cv-03846-JOF (N.D. Ga. Nov. 8, 2011), http://www ftc.gov/os/caselist/1123033/111108skidekidscmpt.pdf.

collection and use practices would be appropriate for a notice and choice regime.

Ohm: Does Congress need to step in and enact privacy legislation, or do you think a self-regulatory solution is workable to provide consumers with the necessary privacy protections?

Brill: I think that legislation would certainly light a fire under industry to put necessary protections in place—that's what a legislative requirement does, right? That being said, I am not sure legislation of this kind is at the top of Congress's agenda so we need to be realistic and continue to urge industry to develop best practices and self-regulatory programs.

Questions from students:

Question: How far do companies need to go in order to be transparent? For example, is it sufficient for a company to say "we're sharing your information" or do they need to say "we're selling your information to third parties?"

Brill: The answer to this question will largely depend on the nature of the personal information. So for example, sensitive data, like health information or financial information, will warrant greater transparency. Certainly, where the Fair Credit Reporting Act[7] ("FCRA") is applicable, there are specific requirements with regard to disclosures about how information is being used. I also point out that the FCRA provides consumers with certain rights to access information about them and to correct it if there are errors. One issue I've been thinking about a great deal is the data broker industry, and trying to ensure that their practices are more transparent—most consumers have no idea who they are or whether they offer the ability for consumers to access the personal information these entities maintain.

Question: Courts have in the past dismissed privacy-related lawsuits due to a failure to demonstrate harm—as in a recent Amazon case.[8] What is the FTC's view on to what extent consumers are harmed by a company's failure to comply with its own privacy policy?

Brill: In private cases, even if there is a clear case of deception, there is generally a need to demonstrate damages, and the difficulty in doing that in an alleged breach of privacy can lead to the dismissal of the case. The FTC and the State AGs do not have the same requirement to demonstrate damages—if a company is engaged in a deceptive practice, that is sufficient to pursue an action under Section 5 of the FTC Act or under the comparable state law.

---

7. Fair Credit Reporting Act, 15 U.S.C. § 1681s(a)(2)(A) (1998).

8. Del Vecchio v. Amazon.com, Inc., No. C11-366-RSL (W.D. Wash. Dec. 1, 2011), http://www.scribd.com/doc/74414398/Amazon-v-Del-Vecchio-11-366-RSL-W-D-Wash-Dec-1-2011.

I'll add that the FTC's authority to pursue privacy-related violations is not limited to deceptive practices. We can also bring actions if a company engaged in an unfair practice—for instance, unfairness is one of the violations we allege in the recent Facebook settlement in connection with some of their challenged practices.[9]

One case worth mentioning here when thinking about harm and the articulation of injury or damages is a case the agency settled with Eli Lilly in 2001.[10] In this case, the company developed a newsletter that Prozac users could subscribe to and, when the company decided to discontinue the newsletter, it notified the subscribers by email—with all the email addresses in the "to" line. No "bcc." So each subscriber could see the email addresses of the other subscribers. Certainly I think we'd all say this caused harm to consumers. The FTC alleged that the company engaged in a deceptive practice, but I do think unfairness would have been an option here as well.

Question: Can you share a bit more about your views about unfairness? Howard Beales has indicated that the FTC's unfairness authority is rather broad and that therefore the agency's existing authority may be sufficient to pursue enforcement actions in order to protect consumers.

Brill: Howard Beales is the former Director of the Bureau of Consumer Protection and an economist. Part of the unfairness test involves determining whether consumers can avoid the injury, and whether the practice is not outweighed by countervailing benefits to consumers or competition. I happen to agree with Howard Beales that the agency can be a bit bolder and more creative in using its unfairness authority in appropriate circumstances. I see Howard regularly, and this is something I frequently discuss with him.

That being said, the agency does face certain limitations in the types of harms it can challenge, even through creative use of our unfairness jurisdiction. So while for example, the agency brought an important case involving peer-to-peer software where the default settings where not privacy protective,[11] the agency may not have had the enforcement tools to challenge the collection by Google of consumer data in connection with Google Streetview.[12] This limitation should be addressed by the passage of additional legislation that will enable the agency to address harms that we currently may not be able to pursue.

---

9. Facebook, Inc., FTC File No. 0923184 (2011).

10. Eli Lilly & Co., FTC File No. 0123214 (2002) (decision and order).

11. FTC, PEER-TO-PEER FILE-SHARING SOFTWARE DEVELOPER SETTLES FTC CHARGES: DEFAULT SETTINGS IN MOBILE FILE-SHARING APP JEOPARDIZED CONSUMERS' PERSONAL FILES (Oct. 11, 2011), http://www.ftc.gov/opa/2011/10/ frostwire.shtm.

12. David C. Vladeck, *Letter to Google*, FTC (October 27, 2010), http://www ftc.gov/os/closing/101027googleletter.pdf.

Editor's Note: Since this event took place, the FTC issued the follow up report to the preliminary framework: Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policy Makers, An FTC Report.[13] ***This report was issued on March 26, 2012.***

13. FTC, *supra* note 1.