Remarks of Commissioner Julie Brill
Before the
Direct Marketing Association:
"*Protecting Consumer Privacy in an Era of Rapid Change*

framework. At the same time, many commenters criticized the slow pace of self-regulation. And many argued that it is time for Congress to enact baseline privacy legislation.

The final report issued today sets forth a revised, final privacy framework. While the final framework adheres to the basic principles laid out in the preliminary report, we have clarified and fine-tuned them, and we have addressed the comments the Commission received.[1]

In the final Report, the Commission calls on Congress to develop baseline privacy legislation. It is time. The Commission is prepared to work with Congress and other stakeholders to craft this legislation. We intend that the final framework we have developed will provide useful guidance to Congress. Baseline privacy legislation will provide businesses with certainty and clear rules of the road, and it will enable industry to act decisively as it continues to innovate.

In terms of our recommendations to industry, we intend the report to serve as best practices that industry can implement to improve the privacy of consumers' information. We urge companies to operationalize the principles laid out in the final framework. And we discuss several self-regulatory efforts. Do Not Track has proceeded well and we encourage all the players to stay in the batter box and swing for another hit to bring home a victory. We also discuss the data broker industry, which needs to follow the example of advertisers and ad networks, and step up to the plate to begin to implement mechanisms to enhance transparency and consumer choice and control.

In the final Report, we clarify and fine-tune our recommendations on best practices. First, as you all know, one of the criteria for providing choice to consumers about use of their data is whether the information is reasonable linkable to an individual, computer or device. In the final report, we clarify that in order for data to be considered not reasonably linkable to an individual or device, companies would need to do three things:

[1] 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.

take reasonable measures to ensure that the data is de-identified;

publicly commit to not attempt to re-identify the data; and

contractually prohibit downstream recipients from attempting to re-identify the data.

This approach both recognizes that we need to pay attention to the blurring lines between PII and non-PII, and yet appropriately encourages industry to deidentify

consistent with the company's relationship with the consumer.[2]

The five "commonly accepted practices" identified in the preliminary report would generally meet this standard, and can be a useful guide, although in some circumstances they may not meet the standard. The Report provides some useful examples of how this "context of the interaction" standard would apply in different circumstances.

In addition to calling on Congress to develop baseline privacy legislation, and calling on industry to operationalize the framework, we also urge industry to accelerate the pace of self-regulation. We've seen considerable progress in some areas – like Do Not Track. But we've seen less progress in other areas, especially from the data broker industry. As a whole, industry still has work to do. And so do we.

To promote important aspects of implementation of our framework, the Commission has five main items on its "to do" list for the coming months.

Do Not Track

On Do Not Track, we will continue to work with the DAA, the browser vendors, the W3C and others to fully implement an easy-to use, persistent, and effective Do Not Track system. Industry has done a lot of good work on Do Not Track. Browsers offered by Microsoft, Mozilla and Apple permit consumers to instruct members of the advertising and data collection ecosystem not to track their activities across websites. Mozilla has also introduced a mobile browser for Android devices that enables Do Not Track.[3] And the DAA has more fully developed its AboutAds program. The DAA program's recent growth and implementation has been significant. At the White House event last month, the DAA committed to honor the choices

[2] Choice is also not required for practices required or specifically authorized by law.

[3] *Do Not Track Adoption in Firefox Mobile is 3x Higher than Desktop*, Mozilla Privacy Blog, (Nov. 2, 2011), http://blog.mozilla.com/privacy/2011/11/02/do-not-track-adoption-in-firefox-mobile-is-3x-higher-than-desktop/.

about tracking that consumers make through settings on their web browsers.[4] I am very pleased to see the DAA's plans to ensure that browser header mechanisms and the AboutAds program work together — that is something I've been

where these apps are available provide this critical information about the apps' collection and use practices.[6] After we released our report about the lack of privacy notices for kids apps, the California Attorney General entered into an agreement with six app platform providers to ensure that privacy policies are displayed so that consumers can read them before they download the apps.[7] That is a good start, but there is still much work to be done in the mobile space. We have called on companies in the mobile app ecosystem to improve the privacy protections in this area, including developing meaningful disclosures and making sure they are provided to consumers.

We have initiated a project to update our business guidance on disclosures. As part of this initiative, we will hold a workshop on May 30th.[8] One of the critical issues we will address is mobile privacy disclosures, and how we can make these disclosures short, effective, and accessible to consumers on small screens. We hope that the workshop will spur further industry innovation and self-regulation in this area.

Data Brokers

In connection with the data broker industry, the Commission supports targeted legislation that would provide consumers with access to information about them held by a data broker. The Report also discusses the Commission's call on data brokers that compile data for marketing purposes to explore creating a centralized website where data brokers could: (1) identify themselves to consumers and describe how they collect and use consumer data, and (2) detail the access rights and other choices they provide with respect to the consumer data they maintain. We will continue our call for greater transparency in the data broker industry. And I will personally be very involved in this effort.

---

[6] *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.

[7] *See Press Release*, Attorney General Kamala D. Harris Secures Global Agreement to Strengthen Privacy Protections for Users of Mobile Applications (Feb. 22, 2012) *available at* http://oag.ca.gov/news/press_release?id=2630.

The Commission will focus its implementation of the report on two other areas as well.

Comprehensive Tracking

The first is comprehensive tracking of consumers' online activities by entities such as ISPs, operating systems, browsers and social media. We recognize the heightened privacy concerns with this kind of tracking and data collection, and we will host a public workshop in the second half of 2012 to delve into these issues.[9]

Enforceable Self-Regulatory Codes

The second is development of enforceable self-regulatory codes. The recent Administration White Paper outlined the need to develop such codes through a multi-stakeholder process.[10] We will participate in the Administration's multi-stakeholder process to develop sector-specific codes of conduct. We will view adherence to such codes favorably in connection with law enforcement actions. And we will enforce industry's promises to abide by such codes.

* * *

I've just outlined five action items, but I probably should have said six because of course, we will continue to bring enforcement actions in appropriate circumstances.

Thank you.

---

[9] *See* Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers, An FTC Report (Mar. 26, 2012) page 73.

[10] *See Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy(Feb. 23, 2012), available at* http://www.whitehouse.gov/sites/default/files/privacy-final.pdf.