

FTC Issues Much-Awaited Consumer Privacy Report

April 2012

On March 26, the Federal Trade Commission (FTC) released its final report on consumer privacy, entitled *Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers* (the Final Report). The 73-page Final Report is a revised version of a December 2010 preliminary staff report (Preliminary Report), which itself flowed out of a multi-year inquiry into whether the FTC's existing approach to consumer privacy was adequate in light of 21st-century technologies and business models.

FTC Chairman Jon Liebowitz characterized the Final Report as laying out what we "must do to make sure that consumers' right of privacy remains robust." In essence, "Consumers should have choice and control." Issuance of the Final Report was also supported by Commissioners Edith Ramirez and Julie Brill. Commissioner J. Thomas Rosch, the only remaining Bush appointee, dissented, expressing concern that the Report relies too heavily on the Commission's "unfairness" authority and recommends practices that could stifle competition.

Establishing a "Privacy Framework"

The Final Report's stated goal is to articulate a "privacy framework" to guide industry, Congress and other policymakers as they consider and respond to consumer privacy concerns. To that end, the Final Report establishes a "privacy framework" of "best practices" that the FTC urges companies to adopt to protect consumers' private information. These would apply in all commercial contexts, not just to online activities. In general, these best practices fall into three categories:

Authors

Brandon J. Moss
Partner
202.719.7554
bmoss@wiley.law

- **Privacy by Design:** Build in privacy at every stage of product development, focusing on data security, reasonable collection limits, sound retention practices and data accuracy;
- **Simplified Consumer Choice:** Give consumers the ability to make decisions about their data at a relevant time and context, including through a Do-Not-Track mechanism; and
- **Transparency:** Make information collection and use practices transparent.

The FTC intends the best practices described in the Final Report to be useful to companies as they develop and maintain privacy and data security processes and useful to Congress as it considers privacy legislation. The FTC indicates that the framework is not intended to serve as a template for law enforcement action or regulation under laws enforced by the FTC.

Changes from the Preliminary Report

The FTC's Final Report evolved somewhat from the December 2010 draft, in response to developments within industry and other government agencies and based upon analysis of the 450 public comments received on the Preliminary Report. For a discussion of the Preliminary Report, see "The FTC Privacy Report Charts a New Regulatory Course But Could Harm Free-Content Websites" (*Privacy In Focus*, January 2011). The FTC identifies three main areas in which the Final Report has changed since the earlier draft:

- **Scope:** Unlike the Preliminary Report, which proposed that the privacy framework apply to all commercial entities collecting or using consumer data that could be reasonably linked to a specific consumer, computer or other device, the Final Report attempts to limit the scope in two ways. First, to alleviate the burden on small businesses, the FTC would not apply the framework to companies that collect only nonsensitive data from fewer than 5,000 consumers a year, provided they do not share the data with third parties. Second, the Final Report also recommends excluding "de-identified" data, by clarifying that data is not "reasonably linkable" to the extent that a company (1) takes reasonable measures to ensure that the data is de-identified; (2) publicly commits not to try to re-identify the data; and (3) contractually prohibits downstream recipients from trying to re-identify the data.
- **Choice:** The Preliminary Report listed five categories of "commonly accepted" information collection and use practices for which companies need not provide consumers with choice. In response to criticisms of this approach, the Final Report sets forth a modified approach that instead focuses on the context of the consumer's interaction with the business. Companies do not need to provide choice before collecting and using consumers' data for practices that are consistent with the context of the transaction, consistent with the company's relationship with the consumer, or as required or specifically authorized by law.
- **Transparency:** The Final Report recommends that Congress consider enacting target legislation to provide greater transparency for, and control over, the practices of information brokers, who, it is asserted, often buy, compile and sell a wealth of highly personal information about consumers without their knowledge or express consent.

What Happens Next?

The Final Report indicates that the FTC plans to promote the implementation of the privacy framework by industry through five main action items, to be addressed over the next year. Specifically, these are:

- **Do-Not-Track:** The FTC will work with groups like the Digital Advertising Alliance and World Wide Web Consortium to complete implementation of an effective Do-Not-Track system.
- **Mobile:** The FTC urges companies providing mobile services to improve privacy protections. To this end, the FTC staff will host a workshop on May 30, 2012, that will address, among other things, mobile privacy disclosures.
- **Data Brokers:** The FTC supports targeted legislation to address data brokers. The FTC also calls on data brokers to explore creating a centralized website where brokers can identify, to consumers themselves, their collection practices and the access rights and other choices provided to consumers.
- **Large Platform Providers:** The FTC intends to host a public workshop in the second half of 2012 exploring comprehensive tracking of consumer online activities by large platforms such as Internet Service Providers, operating systems, browsers and social media.
- **Promoting Enforceable Self-Regulatory Codes:** The FTC will participate in the Department of Commerce's effort to facilitate the development of sector-specific codes of conduct. The FTC will view favorably, in connection with its law enforcement work, adherence to such a code that provides strong protections.

In addition to these initiatives, the Commission says it will call on Congress to enact legislation addressing data security and will ask Congress to consider baseline privacy legislation. It does not contemplate initiating new rulemakings.