The Latest in FTC Privacy Initiatives

On Wednesday, December 1, 2010, the Federal Trade Commission ("FTC") released its long-awaited preliminary report on the protection of consumer privacy, *Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Businesses and Policymakers* (the "Report"). Although the Report does not have the force of law, it is the latest FTC pronouncement indicating that consumer privacy continues to be a growing enforcement priority for the agency. The FTC also intends for the Report to guide organizations' information privacy practices and to inform Congress and other policymakers as they develop new privacy laws and regulations. The FTC is seeking guidance on this preliminary Report, and intends to issue a final report sometime in 2011.

In the Report, the FTC cites new and growing threats to consumer privacy driven by innovations that rely on consumer data, such as cloud computing, social media, behavioral advertising, and mobile and location-enabled devices. In response to these threats, the Report proposes a framework with three core components for entities to protect consumer privacy:

- "**Privacy by Design" –** integrating privacy more fully into products, services, and organizational practices at the earliest stages;
- **Choice –** providing consumers with mechanisms to choose how the organization uses and shares data, including a controversial "Do Not Track" proposal; and
- **Transparency –** increasing transparency of data practices.

The framework described in the Report reiterates certain concrete steps that the FTC believes organizations should take related to choice and transparency and also provides broad guidance that applies to all commercial entities that collect or use consumer data, including entities that do not interact directly with consumers, such as an entity's affiliates and information brokers. The Report covers both online and offline data collection and use. Unlike most privacy regulatory frameworks, this one is *not* limited to personally identifiable information ("PII"). It applies to all consumer data that can be reasonably linked to a specific individual or to a computer or other device. This expanded scope means that the FTC may consider many organizations' current privacy mechanisms that focus solely on PII to no longer provide adequate privacy protection.

For a full text of the report, click here.

A New Privacy Framework

The framework set forth in the Report has three core components:

- **"Privacy by Design" –** According to the Report, given the growing importance of consumer privacy, organizations should integrate privacy concepts into every stage of the development lifecycle for their products and services and should be developing marketing initiatives and data-sharing activities based on privacy guidance from the inception of such projects. The Report also suggests that organizations should develop and maintain comprehensive information programs to protect and

manage consumer data within the organization itself. The Report highlights data security, reasonable collection limits, sound retention practices, and data accuracy as critical program components.

- **Choice –** In the Report the FTC stresses that providing simple and clear mechanisms for consumer choice remains one of the most important mechanisms for preserving consumer privacy. Organizations should offer clear and easy-to-use choice mechanisms at the point when the consumer is making a decision about his or her data, such as at the point of collection. In one of its most controversial recommendations, the FTC proposed a "Do Not Track" mechanism, along the lines of the "Do Not Call" program, such as a persistent web browser setting that allows consumers to block all tracking of their online activities.

  The FTC's suggested framework seeks to streamline consumer choice by identifying "commonly accepted practices" that do not require affirmative consumer consent. The Report lists the following practices as being in this category: fulfillment of requests for products and services, internal operations, fraud prevention, compliance with law enforcement and other legal requirements, and "first party marketing." The Report specifies that while an entity may market directly to its own consumers, it should obtain consumer consent before sharing data for marketing purposes with third parties or even its own affiliates if the affiliate relationship is not clear to consumers through branding or other means. The Report also reiterates previous FTC guidance that enhanced consent may be required for sensitive information, such as information about children, financial and medical information, and precise geolocation data.

- **Transparency –** The Report calls for increased transparency in data practices. The FTC stated that, while privacy policies remain a critical tool for notifying consumers (and regulators) of an entity's privacy practices, the agency believes that, in general, most privacy polices need to be streamlined and simplified. Consistent with long-standing FTC policy, the Report reiterates that an entity must obtain consumer consent before implementing a change in policy that affects previously collected data. It also suggests that organizations should explore mechanisms for providing consumers with access to their data.

What Your Organization Can Do Now

The Report reiterates specific practices that the FTC believes should be followed when handling consumer information and provides generalized guidance. Organizations would be well-served to re-evaluate their own practices relating to consumer information and marketing against each, and to consider how the framework in the Report may shape industry practices going forward. The Report particularly encourages organizations to consider and work to resolve privacy issues at the earliest stages whenever they develop new initiatives, such as marketing initiatives, or other products and services that involve consumer data.

If you would like to learn more about the issues raised by this update, please contact any of the members of our Privacy and Data Security Group listed below.

David McIntosh
Mark Szpak
Ana Francisco
Ed Black
Lisa Ropple
Christine Santariga