FTC Proposes Privacy Framework That Will Impact the Business Model of All Online and Mobile Advertising Companies

December 6, 2010

CLIENT ALERT - DECEMBER 6, 2010

written by David A. Broadwin, Hillary Fitzpatrick, Patrick Connolly

The Federal Trade Commission (FTC) just published its preliminary Staff report setting out its proposed framework for protecting privacy in the digital economy. View the FTC's press release here. The FTC is seeking comments on its proposed framework by January 31, 2011 and expects to issue a final report in 2011.

Every digital media business that attracts advertising revenue online and/or through mobile devices, as well as the venture capital and private equity funds that invest in them, has a stake in the outcome of this proposed framework. It can affect current business models, future financial performance and potential exit opportunities for current and potential companies that rely on collecting data from consumers.

The final report, and possible new regulations and/or federal legislation to follow, will help shape substantive law, enforcement policies and commercial best practices regarding consumer privacy practices that will need to be followed.

Notably, the FTC staff cites flaws in commercially available, privacy-related plug-ins and browser features, and supports a more uniform and comprehensive consumer choice mechanism for online behavioral advertising than currently exists. This is often called "Do Not Track," in a nod to the currently mandated "Do Not Call" registry that restricts the activities of telemarketers. FTC staff identified and requested comment on a number of issues concerning the formulation and adoption of any such "Do Not Track" mechanism.

Other important components of the proposed framework include:

- **Scope:**The proposed framework would apply to all commercial entities that collect or use consumer data that can reasonably be linked to a specific consumer, computer or other device. Here, the FTC staff recognizes the erosion of the distinction between personally- identifiable information (e.g., name, address and social security number) and supposedly anonymous information that may be collected without the knowledge of the web- or mobile device-user.
- **Promotion of consumer privacy:**The proposed framework would require companies to promote consumer privacy and security protections into their daily practices and to consider privacy issues at every stage of design and development of products and services. Suggested steps include:1) providing security for consumer data; 2) limiting data collection to the relevancy of a specific business practice; 3) enforcing sound retention policies; 4) providing assurances of data accuracy; and 5) implementing comprehensive data management procedures throughout the lifecycle of products and services.
- **Consumer choice:**In addition to the "Do Not Track" mechanism described above, the proposed framework would require companies to provide consumers with a notice-and-choice mechanism at the point when the consumer is providing data to the company. This would not be required in the context of commonly- accepted practices, such as order fulfillment or first-party marketing, however.
- **Transparency and Access to Data:**The proposed framework would require vastly- increased transparency with respect to data collection practices and allow for increased consumer access to data collected. As part of implementing this component, the Commission suggests a level of simplification and standardization for currently loosely governed website privacy policies.

Before this framework is submitted in final form to the FTC for a vote by its commissioners, which will accelerate the process further, the FTC is requesting comment by interested parties on a variety of key related issues, including:

- **Scope:** Are there practical considerations that support excluding certain types of companies or businesses from the framework?
- **Substantive Privacy Protections:** What substantive protections should companies provide, and how should the costs and benefits of such protections be balanced?
- **Comprehensive Data Management Procedures:** How can the full range of stakeholders be given an incentive to develop and deploy privacy-enhancing technologies?
- **Consumer Choice; "Do Not Track":**
    1. How should a universal choice mechanism be designed for consumers to control online behavioral advertising?
    2. What are the costs and benefits of offering a standardized uniform choice mechanism to control online behavioral advertising?
    3. What is the likely impact if large numbers of consumers elect to opt out?
    4. Should a universal choice mechanism include an option that allows consumers more granular control over the types of advertising they want to receive and the type of data they are willing to have collected about them?
- **Transparency of Data Practices:** With respect to website privacy notices, is it feasible to standardize the format and terminology for describing data practices across industries? Should companies inform consumers of the identity of those with whom the company has shared data about the consumer, as well as the source of that data?
- **Notifying Consumers of Changes in Data-Use Practices:** What is the appropriate level of transparency and consent for prospective changes to data-handling practices?