ReedSmith

Client Alert

Global Regulatory Enforcement

FTC's Final Order with MySpace Focuses on Privacy by Design and Protection of Unique Device Identifiers

If you have questions or would like additional information on the material covered in this Alert, please contact one of the authors:

Paul Bond
Partner, Princeton
+1 202 414 9223
pbond@reedsmith.com

Amy Mushahwar
Senior Associate,
Washington, D.C.
+1 202 414 9295
amushahwar@reedsmith.com

Christine E. Nielsen
Senior Associate, Chicago
+1 312 207 6459
cnielsen@reedsmith.com

…or the Reed Smith lawyer with whom you regularly work.

On Tuesday, the Federal Trade Commission (FTC) finalized its Consent Order with MySpace, settling allegations that MySpace misrepresented its data use and sharing practices, and its compliance with the U.S.-EU Safe Harbor Framework in its privacy policy. In a 4-0-1 decision, with Commissioner Maureen Ohlhausen not participating, the Commission voted to accept the proposed order and enjoin MySpace from practices that violate the FTC Act.

On May 8, the FTC simultaneously released its Complaint and Proposed Order against MySpace and opened a 30-day comment period on the proposed resolution. The FTC alleged that MySpace's sharing of its "Friend ID," a persistent unique numerical identification number assigned to each MySpace user, violated its own privacy policy representations that it did not share personal information without the user's permission. MySpace had designated the Friend ID as "basic profile information" that users could not hide from public view, but the FTC alleged that the Friend ID could be linked to a user's full name, and if the user had designated his or her profile to be open to MySpace users, the Friend ID could be linked to other personal data on that user. The FTC noted that because of MySpace's data-sharing practices with affiliated and unaffiliated advertising networks,

> a third-party advertiser could take simple steps to get detailed information about individual users. For example, a third party advertiser could use the Friend ID to: a. visit the user's personal profile on the MySpace website, to obtain his or her real name and other publicly available information; and b. combine the user's real name and other personal information with that advertiser's tracking cookie and the history of websites the user has visited that it contains.

The FTC alleged that MySpace represented in its privacy policy that it did not share user personal information with unaffiliated third parties or advertisers without giving notice and obtaining consent from users, when in fact the use of the Friend ID, which allowed access to personal information, was conducted without providing notice in the privacy policy or obtaining consent. Such collection and use practices also meant that MySpace's representations about its compliance with the U.S.-EU Safe Harbor Privacy Principles were false and misleading, according to the FTC.

The Order requires MySpace to establish, implement, and thereafter maintain a comprehensive privacy program. In October 2011, the FTC entered into a final consent order with Google over Google's Buzz program. The Google Order represented the first time the FTC required a company to implement a "Comprehensive Privacy Program" and not an "Information Security Program." This MySpace Order continues the trend of codifying the privacy by design concept, discussed in both the FTC's preliminary staff report on privacy in December 2010, and in the final report issued last March, requiring the company to assess privacy risks related to the development of new products and services, and to integrate controls to address those risks.

Of additional note, the program must protect the privacy of covered information, which as defined includes: name; address; email address; telephone number; photos and videos; IP address, device ID or other persistent identifier; list of contacts; or physical location. IP addresses, user IDs, unique device IDs, or other persistent identifiers have not historically been thought of as "personally identifiable information," but their inclusion in the definition of covered information is consistent with the FTC's decision to apply its privacy framework to data that is reasonably linkable to a specific consumer, computer, or device. This focus on unique device identifiers and their combination with other pieces of data will likely only intensify, as policy discussions on privacy by design and other concepts such as Do Not Track continue at the federal level.