Facebook Settlement with the FTC Includes Stringent Privacy Requirements

Dana B. Rosenfeld

November 30, 2011

Facebook has agreed to settle Federal Trade Commission ("FTC") charges alleging that the social network company engaged in deceptive practices that enabled third-party access to Facebook users' private information, including personal history, photos, videos, and Friend Lists, without providing users with adequate notice or obtaining their prior consent.

The proposed settlement, which would impose privacy requirements that are similar to those in the FTC's settlement with Google that became final in October 2011, follows complaints over Facebook's privacy practices that were filed with the FTC in December 2009 by the Electronic Privacy Information Center ("EPIC") and a coalition of consumer groups.

The FTC Complaint

The FTC's administrative complaint alleges a number of violations of Section 5(a) of the FTC Act, which prohibits deceptive or unfair acts or practices in or affecting commerce, including allegations that (1) Facebook users' personal information was made publicly-available despite repeated representations by Facebook that such information would remain private; (2) applications ("Apps") available through the Facebook platform could access personal information without Facebook users' knowledge or consent; and (3) Facebook falsely stated that it complied with the United States – European Union ("EU") Safe Harbor Framework:

- **Personal Information Available to Third-Parties following Unilateral Changes to Privacy Settings**: The FTC alleged that Facebook users were not given adequate notice that certain private information would become publicly-available following changes to Facebook's privacy settings, and were not given meaningful choice about whether they agreed to the public status of their information. Further, the FTC alleged that, despite statements by Facebook that personal information was not shared with advertisers, users' User ID information became available to an advertiser whenever a user clicked on an advertisement. The FTC also alleged that personal photos and videos remained available on Facebook even after such content was deleted by a user or the user deactivated his or her Facebook account.

- **Apps Access to Private Information**: The FTC alleged that Apps available on the Facebook platform could access users' personal information even when the information was unrelated to the operation of the app or when certain information was designated by users as "Friends Only." The FTC also alleged that Facebook's "Verified Applications" program was deceptive as it did not employ verification procedures or security safeguards that exceeded the level of protection applied to any other App on the Facebook platform.

- **Noncompliance with U.S.–EU Safe Harbor Framework**: The FTC alleged that, despite representations within Facebook's privacy policy that the company complied with the U.S.-EU Safe Harbor Framework, Facebook's privacy practices violated the U.S. Safe Harbor Privacy Principles of Notice and Choice.

Terms of the Proposed Settlement

The proposed settlement, which is subject to public comment through December 30, 2011, imposes robust requirements on Facebook, including the following:

- Before sharing user information with a third party in a manner that materially exceeds the restrictions imposed by a users' privacy settings, Facebook must:
    - Disclose (1) the information that will be shared, (2) the identity or categories of the third parties that will receive the information, and (3) that such sharing exceeds the restrictions imposed by the users' privacy settings. Notably, this disclosure must be separate from any "end user license agreement," "privacy policy," or "terms of use;" and
    - Obtain express affirmative consent to the sharing from the user.
- Facebook must ensure that personal information cannot be accessed by a third-party within 30 days after a user deletes such information or terminates his or her Facebook account.
- Facebook must develop, implement, and maintain a written comprehensive privacy program including designated employees responsible for the program; identification of reasonably foreseeable risks and safeguards used to mitigate risks; and establishing steps to select and retain service providers.
- Facebook must hire a third party privacy and data security professional to conduct assessments of Facebook's practices every two years for the next twenty years.

What this Means for Business

This FTC action is the latest reminder to businesses that handle consumer information that they must carefully evaluate whether their privacy practices are consistent with promises made in their policies and whether they provide adequate disclosures and obtain meaningful consent from customers when these practices change. With this high-profile settlement, the FTC has signaled that it will continue its aggressive privacy-related enforcement activity regarding the handling of consumers' personal information.

This post was written by Dana Rosenfeld and Alysa Z. Hutnik.