

Privacy and Data Protection Alert

FTC Announces Google Buzz Settlement: Privacy Implications for Other Companies

April 1, 2011

In a groundbreaking enforcement action, the Federal Trade Commission (FTC) this March reached a [settlement with Google Inc.](#) over charges that Google violated Section 5(a) of the FTC Act and U.S.-E.U. Safe Harbor Principles by using deceptive tactics and violating its own privacy policy. Most significantly, this settlement marks the first time the FTC has required a company to implement a comprehensive privacy regime based upon alleged deceptive practice. While the FTC has imposed similar structural privacy requirements in past matters involving security breaches, this case represents the FTC's first effort to impose, through an enforcement action, its current preferred policy position: the "privacy by design" concept. Under that concept, companies are required to consider privacy issues in every aspect of their businesses and put in place policies and procedures to implement the baseline goals of notice, choice, security and access.

This precedent, as well as a groundswell of legislative activity, demonstrates the growing risks for companies that collect, use and disclose consumer data as part of their business practices. While this particular settlement will be binding only on Google, it presents a roadmap to the practices the FTC expects similarly situated companies to follow. Thus, it is now more imperative than ever that companies analyze their data privacy practices to ensure that they are in compliance with various laws and regulations, including this latest guidance from the FTC.

Background of the FTC Complaint

In its [complaint](#) against Google, the FTC alleged that the Internet search giant used deceptive tactics to get people to use its social networking tool, Google Buzz. In February 2010, in an effort to compete with Facebook and Twitter, Google launched Buzz, an add-on to its Gmail e-mail service that allows Gmail users to post comments on various Google applications and share them with other Gmail users. In order to populate the new network quickly, Google automatically set up Gmail users with "followers" based on the people they e-mailed and chatted with most frequently. The problem was that Google allegedly opted in all Gmail users automatically and did not give users effective means to opt out of the new product or to keep their e-mail lists private. These practices also contradicted Google's historical privacy policies.

According to the FTC, "[t]he setup process for Gmail users who enrolled in Buzz did not adequately communicate that certain previously private information would be shared publicly by default" and "the controls that would allow the user to change the defaults were confusing and difficult to find."¹ For instance, the FTC alleged that there were no disclosures on the Buzz welcome screen that information posted in Buzz was, by default, public or that the entire list of "followers" would be posted on a user's public Google profile, thus making visible to anyone a list of people the user e-mailed or chatted with most frequently.

¹ FTC complaint, page 3, point 9.



At the time of launching Buzz, Google's privacy policy stated: "When you sign up for a particular service that requires registration, we ask you to provide personal information. If we use this information in a manner different than the purpose for which it was collected, then we will ask for your consent prior to such use."² In this case, the FTC alleged that Google used user information it gathered for Gmail to build a social network that had nothing to do with e-mail, without prior notice or the opportunity for users to consent, thus violating its own privacy policy.

Additionally, the complaint alleged that Google violated the U.S.-E.U. Safe Harbor Privacy Principles, making this a first-ever substantive Safe Harbor enforcement action by the FTC. The Privacy Principles were developed by the U.S. Department of Commerce and the European Commission in order to bridge differences in approach to privacy protection between the United States and the European Union and provide a means for U.S. companies to comply with EU Directive 95/46/EC on the protection of personal data. Under the FTC Act, a company's failure to abide by commitments to implement the Safe Harbor Privacy Principles may itself be considered a deceptive practice, and the FTC has the power to enforce it. The FTC alleged that Google violated the Principles by failing to provide its European users with a notice of the proposed new use for the information it had collected, constituting a violation of the Section 5 of the FTC Act.

Settlement and Consent Order

The settlement contains several major requirements, including a prohibition against misrepresentation, a requirement to provide notice and obtain consent from users, and mandatory implementation of a comprehensive privacy program.

First, Google is expressly prohibited from misrepresenting the extent to which it maintains and protects any "covered information" (which, in addition to user's name, physical and e-mail addresses and telephone numbers, includes an individual's list of contacts, physical location and IP address). This prohibition includes (i) misrepresentations regarding Google's purposes for collecting and using such information, (ii) the extent to which users can exercise control over the collection and use of their data and (iii) Google's compliance with any privacy program, such as the U.S.-E.U. Safe Harbor Framework.

Second, before sharing its users' covered information with any third party, the company must provide users with specific disclosure and obtain "express affirmative consent" from the users unless such consent was previously given for the specific use.

Finally, Google was ordered to create and maintain a comprehensive privacy protection program "that is reasonably designed to: (1) address privacy risks related to the development and management of new and existing products and services for consumers, and (2) protect the privacy and confidentiality of covered information."³ This privacy program must be documented, and the privacy controls must include, among other things, identification and assessment of reasonably foreseeable material risks to the privacy of covered information, regular testing or monitoring of the effectiveness of privacy controls and procedures and a requirement that service providers, by contract, implement and maintain appropriate privacy protections. Importantly, as a part of this comprehensive privacy compliance program, Google will have to undergo audits of its privacy compliance practices by an independent third-party professional every other year for the next 20 years. The auditor will have to be approved by the FTC and will assess privacy controls implemented by Google, including their appropriateness to Google's size and complexity, and certify that such controls are of sufficient effectiveness to reasonably protect the privacy of users' information. This settlement provision is the first of its kind in FTC enforcement actions.

This unprecedented settlement and consent order technically will apply only to Google. However, it also signals heightened attention by the FTC to the protection of consumer privacy. The precedent will likely affect data companies, advertisers, and online retailers, among others, especially given that the FTC views these measures as "good business

² FTC complaint, page 2, point 6(b).

³ Proposed settlement, p.4, at III.

practices that we'd expect to see widely followed across the industry.”⁴ In light of these developments, companies that use consumer data would be well-advised to assess their privacy protection measures and procedures, making sure that they comply with various regulatory requirements, including the FTC guidelines and U.S.-E.U. Safe Harbor framework requirements.

CONTACT INFORMATION

If you have any questions concerning this alert, please contact —

Daniel F. McInnis
dmcinnis@akingump.com
202.887.4359
Washington, D.C.

Elaine M. Laflamme
elaflamme@akingump.com
212.872.8039
New York, NY

Jo-Ellyn Sakowitz Klein
jsklein@akingump.com
202.887.4220
Washington, D.C.

Ausra Laurusaite-Kromelis
alaurusaitekromelis@akingump.com
214.969.2878
Dallas, TX

⁴ Politico.com article quoting Jessica Rich, deputy director of the FTC's Bureau of Consumer Protection, <http://www.politico.com/news/stories/0311/52257.html>.