

Morrison & Foerster Client Alert.

April 4, 2011

Proposed Settlement With Google Sets New Precedents and Highlights the FTC's Privacy Priorities

By **D. Reed Freeman, Julie O'Neill, and Kimberly S. Robinson**

The Federal Trade Commission ("FTC" or "Commission") recently announced a settlement in a privacy enforcement action that sets new precedents and sends new signals to privacy professionals about current FTC expectations. The case against Google for its Google Buzz social medial service rollout is the Commission's first case alleging substantive violations of the U.S.-EU Safe Harbor provisions and its first settlement requiring the implementation of a comprehensive "privacy by design" program for all future products and services and also requiring biannual, independent privacy audits for twenty years. The settlement also requires Google to get opt-in consent for secondary uses or disclosures of data.

The settlement is now open for public comment, which the FTC will receive until May 2, after which it will determine whether to make the settlement final or alter its requirements.

THE FTC'S COMPLAINT

The Commission's complaint contains two principal allegations. First, the Commission alleged that Google violated the following statement in its privacy policy:

"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."

In particular, the FTC alleged that Gmail users' personal information was made public through the Google Buzz social marketing service without their consent, and even sometimes when the users tried to opt out of the Buzz service. The FTC further alleged that the controls and opt-outs were confusing and in some cases ineffective.

Beijing

Paul D. McKenzie 86 10 5909 3366
Jingxiao Fang 86 10 5909 3382

Brussels

Karin Retzer 32 2 340 7364
Joanne Lopatowska 32 2 340 7365

Hong Kong

Gordon A. Milner 852 2585 0808
Nigel C.H. Stamp 852 2585 0888

Los Angeles

Mark T. Gillett (213) 892-5289
Michael C. Cohen (213) 892-5404
David F. McDowell (213) 892-5383
Russell G. Weiss (213) 892-5640

London

Ann Bevitt 44 20 7920 4041
Anthony Nagle 44 20 7920 4029
Chris Coulter 44 20 7920 4012

New York

Joan P. Warrington (212) 506-7307
John F. Delaney (212) 468-8040
Madhavi T. Batliboi (212) 336-5181
Suhna Pierce (212) 336-4150
Marian A. Waldmann (212) 336-4230
Miriam Wugmeister (212) 506-7213
Sherman W. Kahn (212) 468-8023

Northern Virginia

Daniel P. Westman (703) 760-7795
Timothy G. Verrall (703) 760-7306

Palo Alto

Bryan Wilson (650) 813-5603
Christine E. Lyon (650) 813-5770

San Francisco

Roland E. Brandel (415) 268-7093
James McGuire (415) 268-7013
William L. Stern (415) 268-7637
Jim McCabe (415) 268-7011

Tokyo

Daniel P. Levison 81 3 3214 6717
Gabriel E. Meister 81 3 3214 6748
Jay Ponazecki 81 3 3214 6562
Toshihiro So 81 3 3214 6568
Yukihiko Terazawa 81 3 3214 6585

Washington, D.C.

Andrew M. Smith (202) 887-1558
Cynthia J. Rich (202) 778-1652
Julie O'Neill (202) 887-8764
Nathan David Taylor (202) 778-1644
Obrea O. Poindexter (202) 887-8741
Reed Freeman (202) 887-6948
Richard Fischer (202) 887-1566
Kimberly Strawbridge Robinson (202) 887-1508

Client Alert.

The Commission also alleged that Google misrepresented its compliance with its Safe Harbor certification because (according to the FTC) the company failed to give consumers notice and choice before using their information for a purpose different from that for which it was collected. In the past, the Commission has charged companies with deception for claiming that they were certified under the Safe Harbor program when they actually were not. This action is different. The Commission here alleged that Google failed to comply with the substantive “Notice” and “Choice” principles required of certified companies. Specifically, Google allegedly failed to give users of its Gmail service notice before using the information it collected from them for a purpose other than that for which it was originally collected. Because Google’s Safe Harbor certification represented to consumers that it was compliant with Safe Harbor principles, the Commission alleged that its failure to fully comply with them was deceptive and in violation of Section 5 of the FTC Act.

THE PROPOSED SETTLEMENT AGREEMENT

Privacy by Design

The proposed settlement agreement with Google includes a “privacy by design” provision that requires Google to implement a comprehensive privacy program that addresses the privacy risks related to the development of new products and generally protects the privacy of consumer information. Specifically, the program must:

- (1) designate a responsible employee for privacy matters;
- (2) identify reasonably foreseeable risks that may result in the unauthorized collection, use, or disclosure of consumer information (including an assessment of employee training and product design, development, and research);
- (3) design and implement controls to address these risks; and
- (4) develop and implement reasonable steps to select service providers that will adequately protect consumer privacy.

This is the first time that the FTC has ordered such relief. We do not expect it to be the last. The take-away is that the FTC is developing “common law by settlement decree” by incorporating these elements into a settlement addressing Section 5 allegations.

Biannual Audits for 20 Years

The proposed settlement agreement also includes a provision requiring Google to undergo an independent privacy audit every other year for 20 years. We expect to see this provision become another staple of privacy settlements going forward.

Opt-In

To address Google’s alleged failure to get users’ consent as promised in its privacy policy, the settlement requires Google to obtain users’ opt-in consent before sharing their information with third parties if Google changes its products or services in a way that results in information sharing that is contrary to any privacy promises made when the user’s information was collected.

This requirement is significant. As Commissioner Rosch points out in his concurrence, this provision “applies whenever Google engages in any ‘new or additional sharing’ of previously collected personal information ‘with any third party’ for the next twenty years, not just any ‘material’ new or additional sharing of that information.”

The opt-in requirement is startling because it goes beyond what Google actually promised. Google only promised in its privacy policy to obtain consent, which would have been satisfied by providing an opt-out consent option. As part of this settlement agreement, Google is agreeing to request opt-in consent. Whether this type of Draconian relief will find its way into future settlement agreements is unclear, but it does underscore that the Commission is serious about making sure

Client Alert.

companies live up to not just their privacy promises as written, but to interpretations of those promises that may go beyond what the company may have intended to convey.

Safe Harbor Provisions

The settlement also marks the first time that the Commission has held a company accountable for its alleged failure to comply with substantive privacy provisions of the U.S./EU Safe Harbor framework. These charges serve as an important reminder that certification to the Safe Harbor is serious and is a representation to consumers, actionable by the Commission if the representation is false. The settlement bars Google from misrepresenting the privacy or confidentiality of individuals' information or misrepresenting compliance with the U.S.-EU Safe Harbor or any other privacy, security, or compliance programs.

It is unclear whether the opt-in provision is also meant to remedy Google's alleged failure to comply with the substantive provisions of the Safe Harbor program. It is important to note that the Safe Harbor requires opt-out choice (not opt-in) for new uses of non-sensitive personal information. Opt-in choice is required only for sensitive personal information. We expect commenters to focus on this requirement, in hopes of the Commission clarifying that it has not sought to apply an important substantive change in the Safe Harbor requirements in the form of a settlement agreement.

PRACTICAL IMPLICATIONS

The FTC's complaint and settlement agreement in this matter are noteworthy because they break new ground in privacy matters and send a number of signals to the market. It is not unusual for the Commission to express its expectations through a settlement agreement, but it is unusual for it to express so many new rules simultaneously. In this case, the Commission believes that it has put the market on notice that it will interpret privacy promises broadly and apply strong injunctive relief where it finds that the promises are untrue; that it will look for and prosecute companies' failures strictly to abide by the principles underlying their Safe Harbor certifications; that it has a new template for privacy settlement agreements that require a "privacy by design" approach and biannual audits for 20 years (and, consequently, that it is beginning to consider privacy by design as a Section 5 requirement); and, fundamentally, that it intends to remain vigilant in holding companies to their promises, especially when they involve consumers' control of, and choices regarding, their personal information.

IN LIGHT OF THIS PROPOSED SETTLEMENT COMPANIES SHOULD:

- Ensure that privacy policies accurately reflect current practices;
- If intending to use personal information for a purpose that is different than the purpose for which the information was collected, give consumers choice as provided in the privacy policy, using a broad interpretation of the privacy policy as a guide;
- Begin to incorporate the "privacy by design" elements laid out in the Commission's order, including:
 - Designating an employee responsible for privacy;
 - Training employees on privacy policies;
 - Identifying potential violations of policies when developing new products and services, or enhancements to existing products or services; and
 - Identifying reasonably foreseeable risks to access, use, and disclosures of consumers' information that are inconsistent with the reasons for which they were provided by the consumer;
- If Safe Harbor certified, ensure compliance with all of the Safe Harbor obligations.

Client Alert.

About Morrison & Foerster:

We are Morrison & Foerster—a global firm of exceptional credentials in many areas. Our clients include some of the largest financial institutions, investment banks, Fortune 100, technology and life science companies. We've been included on *The American Lawyer's* A-List for seven straight years, and *Fortune* named us one of the "100 Best Companies to Work For." Our lawyers are committed to achieving innovative and business-minded results for our clients, while preserving the differences that make us stronger. This is MoFo. Visit us at www.mofo.com.

Because of the generality of this update, the information provided herein may not be applicable in all situations and should not be acted upon without specific legal advice based on particular situations.