December 8, 2011

Proposed Settlement with Facebook Underscores the FTC's Privacy Priorities

By D. Reed Freeman, Julie O'Neill, and Nicholas A. Datlowe

On November 29, 2011, the Federal Trade Commission ("FTC") announced a proposed order against Facebook that builds upon the recommendations it made in the draft privacy report it released a year ago, as well as on precedents it set in the order it recently imposed on Google Inc.[1] Any business that collects personal information from consumers should pay close attention to this action because it makes it clear that:

- ***The FTC will continue to remain vigilant in holding companies to their privacy promises.*** It will pay particular attention when those promises involve consumers' choices regarding their personal information, and it will continue to look for and prosecute companies' failures to abide by the principles underlying their US/EU Safe Harbor certifications;
- ***The FTC will continue to require opt-in consent for material changes to a company's privacy practices.*** This is not new, but it is worth repeating that the FTC has not backed away from its assertion that, when a company changes its privacy practices in a material way, it must obtain consumers' opt-in consent to those changes before applying them retroactively (*i.e.*, to information already collected);
- ***The FTC has a robust new template for privacy orders.*** It will continue to impose onerous injunctive relief on companies that do not abide by their own privacy promises, including the obligation – even where there has been no alleged data breach – to obtain an independent privacy audit every other year for 20 years; and
- ***The FTC will continue to require companies subject to a privacy order to implement and maintain a comprehensive "privacy by design" program and, in fact, may begin to expect this from all companies.*** In its 2010 draft

[1] *See* http://www.ftc.gov/opa/2011/11/privacysettlement.shtm. The FTC's draft privacy is discussed at http://www.mofo.com/files/Uploads/Images/101203-Do-not-track-list.pdf, and its order against Google (brought in connection with its Google Buzz social media service) is discussed at http://www.mofo.com/files/Uploads/Images/110404-FTC-Privacy-Priorities.pdf.

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

Brussels
Joanna Łopatowska 32 2 340 7365
Karin Retzer 32 2 340 7364

Hong Kong
Gordon A. Milner 852 2585 0808

London
Ann Bevitt 44 20 7920 4041
Deirdre Moynihan 44 20 7920 4164
Anthony Nagle 44 20 7920 4029

Los Angeles
Michael C. Cohen (213) 892-5404
David F. McDowell (213) 892-5383
Purvi G. Patel (213) 892-5296
Russell G. Weiss (213) 892-5640

New York
Madhavi T. Batliboi (212) 336-5181
John F. Delaney (212) 468-8040
Sherman W. Kahn (212) 468-8023
Mark P. Ladner (212) 468-8035
Michael B. Miller (212) 468-8009
Suhna N. Pierce (212) 336-4150
Marian A. Waldmann (212) 336-4230
Miriam H. Wugmeister (212) 506-7213

Northern Virginia
Daniel P. Westman (703) 760-7795

Palo Alto
Anna Ferrari (650) 813-5681
Christine E. Lyon (650) 813-5770
Bryan Wilson (650) 813-5603

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

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
Yukihiro Terazawa 81 3 3214 6585

Washington, D.C.
Nicholas A. Datlowe (202) 887-1590
Richard Fischer (202) 887-1566
D. Reed Freeman, Jr. (202) 887-6948
Julie O'Neill (202) 887-8764
Obrea O. Poindexter (202) 887-8741
Cynthia J. Rich (202) 778-1652
Kimberly Strawbridge Robinson (202) 887-1508
Robert A. Salerno (202) 887-6930
Andrew M. Smith (202) 887-1558
Nathan David Taylor (202) 778-1644

privacy report, the FTC proposed that businesses make privacy and data security a routine consideration by adopting a "privacy by design" approach. The report has not yet been finalized, but that has not stopped the FTC from moving this proposal closer toward becoming a legal requirement by way of its enforcement actions against Google and Facebook (the FTC often expresses its "expectations" of industry through settlement agreements). We take the inclusion of a "privacy by design" requirement in both orders to mean that the FTC thinks that all businesses should adopt such procedures and that, eventually, the FTC is likely to view a failure to have them as deceptive and/or unfair, in violation of the FTC Act.

The proposed order would settle charges that a variety of Facebook's information practices were deceptive or unfair. Highlights of the complaint and proposed order are summarized below. The proposed order is open for public comment until December 30, 2011, after which the FTC will determine whether to make it final or modify its requirements.

THE FTC'S COMPLAINT

The FTC's complaint against Facebook contains eight counts, all of which underscore the theme repeated in the FTC's privacy enforcement actions over the years: businesses must comply with the privacy promises that they make to consumers. Here, the FTC has alleged that Facebook failed to comply with promises it made to its users in a variety of contexts over time. Specifically:

- **Facebook's privacy settings: access to personal information.** Facebook promised its users that they could limit the categories of those who could access their personal information through the choices that they made in their Profile Privacy Pages. In fact, according to the FTC, users' choices were meaningless because Facebook permitted third-party applications used by a user's Facebook friends to access the user's personal information – including marital status, birthday, town, schools, jobs, photos, and videos – regardless of the privacy settings chosen by the user. The FTC has therefore alleged that the company's representations were deceptive.

- **Facebook's privacy settings: overriding user choice.** Two counts in the FTC's complaint address privacy policy changes that Facebook made in December 2009 – changes that Facebook claimed would not only give users more control over their personal information but also allow them to keep their existing privacy settings. According to the FTC, contrary to those promises, some information designated by users as private (such as a friend list) was actually made public under the new policy. The FTC has charged that this was deceptive because Facebook overrode users' existing privacy choices without adequate disclosure. The FTC has further charged that the change constituted an unfair practice because Facebook retroactively applied material changes to personal information it had already collected from users without first obtaining their consent. In the FTC's view, the practice met the standard for unfairness because it "has caused or has been likely to cause substantial injury to consumers, was not outweighed by countervailing benefits to consumers or to competition, and was not reasonably avoidable by consumers."

- **Scope of applications' access to user information.** The FTC has alleged that, for more than three years from the debut of applications on the Facebook platform, Facebook deceived its users about the scope of the profile information accessible to apps. Specifically, Facebook told users that an app would have access to only the information "that it requires to work." The FTC has charged that this promise was deceptive because, in many instances, Facebook gave apps unrestricted access to user profile information, including information that they did not need to operate.

- **Advertisers' receipt of user information.** According to the FTC's complaint, Facebook represented to its users numerous times that it would not share their information with advertisers without the users' consent. For instance, in its Statement of Rights and Responsibilities, Facebook promised: *"We don't share your information with advertisers unless you tell us to . . . Any assertion to the contrary is false. Period … we never provide the advertiser any names or other information about the people who are shown, or even who click on, the ads."* The FTC has alleged that this representation and others like it were deceptive because, from at least September 2008 until the end of May 2010, Facebook's site was designed and operated such that the User ID of a user who clicked on an advertisement was, in many cases, shared with the advertiser.

- **Facebook's "Verified Apps" program.** Facebook promised its users that, under its "Verified App" program, it reviewed apps so as to "offer extra assurances to help users identify applications they can trust – applications that are secure, respectful and transparent, and have demonstrated commitment to compliance with [Facebook] policies." According to the FTC, however, because Facebook did not take any steps to verify an app in any of these ways, its promise was deceptive.

- **Photo and video deletion.** Facebook told users that when they deactivated or deleted their accounts, their photos and videos would be inaccessible to others. The FTC has alleged, however, that Facebook continued to serve up the photos and videos of both deactivated and deleted accounts to third parties, and, accordingly, the company's promises were deceptive.

- **Compliance with the US-EU Safe Harbor Framework.** The FTC has alleged that Facebook misrepresented its compliance with its Safe Harbor certification because – as described above – it failed to give its users notice and choice before using their information for a purpose different from that for which it was collected, in violation of the "Notice" and "Choice" principles required of Safe Harbor certified companies. Because Facebook's Safe Harbor certification represented to consumers that it was compliant with the principles, the FTC has charged that its failure to comply with them was unfair or deceptive.

THE PROPOSED SETTLEMENT AGREEMENT

No Privacy or Security Misrepresentations

Like all FTC orders settling charges of deception, the proposed order would prohibit Facebook from future misrepresentations. Specifically, the order would enjoin Facebook from express and implied misrepresentations about how it maintains the privacy or security of users' information, including: (1) the extent to which a user can control the privacy of his or her information; (2) the extent to which Facebook makes user information available to third parties; and (3) the extent to which Facebook makes information accessible to third parties after a user has terminated his or her account.

Opt-In Consent for New Disclosures

The proposed settlement agreement would require Facebook to obtain users' opt-in consent before sharing their information with a third party in a way that materially exceeds the restrictions imposed by the users' privacy settings. This obligation ratifies a requirement that the FTC first imposed against Gateway Learning in 2004[2] and which it has

[2] See http://www.ftc.gov/opa/2004/07/gateway.shtm.

repeated numerous times since then:[3] a company that makes a material change to its privacy practice must obtain affected individuals' opt-in consent to that change before applying it retroactively (*i.e.*, to information already collected). The proposed order specifies the way in which Facebook must obtain such consent. It must: (1) clearly and conspicuously disclose to the user, separate and apart from any privacy policy or similar document (a) the categories of information that will be disclosed, (b) the identity or categories of the recipients, and (c) the fact that such sharing exceeds the restrictions imposed by the user's privacy settings; and (2) obtain his or her affirmative express consent to the disclosure.[4]

Deletion of "Deleted" Content

The proposed settlement would require Facebook to implement procedures reasonably designed to ensure that the information of a user who has deleted his or her information or deleted or terminated his or her account is not accessible by any third party.

Privacy by Design

Like the FTC's order against Google, the proposed Facebook order includes a "privacy by design" provision that would require the company to implement and maintain a comprehensive privacy program that (1) addresses the privacy risks related to the development and management of both new and existing products and services, and (2) protects the privacy of user information. Specifically, Facebook would have to:

- designate a responsible employee(s);
- identify reasonably foreseeable, material risks that could result in the unauthorized collection, use, or disclosure of user information;
- design and implement reasonable controls and procedures to address identified risks and regularly test them;
- develop and implement reasonable steps to select service providers that will adequately protect user privacy and contractually require them to maintain appropriate protections; and
- evaluate and adjust the privacy program in light of the testing required by it, any material change to Facebook's operations, or any other circumstances that may have a material impact on the program's effectiveness.

[3] *See, e.g.,* the FTC's draft privacy report, "Protecting Consumer Privacy in an Era of Rapid Change," issued in December 2010 and available at http://www.ftc.gov/os/2010/12/101201privacyreport.pdf (discussed at http://www.mofo.com/files/Uploads/Images/101203-Do-not-track-list.pdf) and its staff report "Self-Regulatory Principles for Online Behavioral Advertising," issued in February 2009 and available at http://www.ftc.gov/os/2009/02/P085400behavadreport.pdf.

[4] It is not clear whether the proposed order's requirement that Facebook obtain a user's opt-in consent to a material change applied retroactively is intended to remedy the company's alleged failure to comply with the Safe Harbor's Notice and Choice principles, or instead only to impose the standard the FTC requires under US law. If it is intended to cover the alleged Safe Harbor violations, then it goes beyond the Safe Harbor principles, which require opt-out (not opt-in) choice for new uses of non-sensitive personal information. The same question arose in connection with the FTC's Google Buzz order, and we have not seen any clarification from the FTC.

In the draft privacy report that it released a year ago, the FTC proposed that businesses make privacy and data security a routine consideration by adopting a "privacy by design" approach.[5] Although it has not yet finalized the report, the FTC has moved this proposal closer to becoming a legal requirement through both this proposed order and its recent order against Google. The FTC often expresses its expectations of industry through a settlement agreement. For this reason, we take the inclusion of a "privacy by design" requirement in both orders to mean that the FTC thinks that all businesses should adopt such procedures and that, eventually, the FTC is likely to view a failure to have them as deceptive and/or unfair, in violation of the FTC Act.

Biannual Audits for 20 Years

The proposed settlement agreement would require Facebook to obtain an independent privacy audit every other year for 20 years. In light of the fact that this is the second time that the FTC has imposed such relief this year (after the Google matter), we expect that it, like the "privacy by design" provision, will become a staple of FTC privacy settlements.

Safe Harbor Provisions

The proposed settlement marks the second time that the FTC has held a company accountable for its alleged failure to comply with substantive privacy provisions of the US/EU Safe Harbor framework. (The first was in the Google action.) The charges serve as an important reminder that Safe Harbor certification constitutes a representation to consumers that, if false, is actionable. The proposed order would bar Facebook from misrepresenting its compliance with the Safe Harbor or any other privacy, security, or other compliance program.

CONCLUSION

The FTC's complaint and proposed order against Facebook are noteworthy because they reinforce the precedents that the FTC set in its action against Google, thereby sending the following unmistakable signals to the market:

- The FTC will continue to hold companies to their privacy promises and apply strong injunctive relief where it finds that the promises are false;
- The FTC continues to believe that a company must obtain affected consumers' affirmative consent to new privacy practices applied retroactively;
- The FTC will continue to look for and prosecute companies' failures to abide by the principles underlying their Safe Harbor certifications;
- The FTC has a new template for privacy settlement agreements – one that requires a "privacy by design" approach to business, as well as independent biannual audits for 20 years; and
- The FTC is beginning to consider privacy by design as a requirement under Section 5 of the FTC Act, which prohibits unfair and deceptive acts and practices.

[5] *See* http://www.mofo.com/files/Uploads/Images/101203-Do-not-track-list.pdf.

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.

Morrison & Foerster has a world-class privacy and data security practice that is cross-disciplinary and spans our global offices. With more than 60 lawyers actively counseling, litigating, and representing clients before regulators around the world on privacy and security of information issues, we have been recognized by *Chambers* and *Legal 500* as having one of the best domestic and global practices in this area.

For more information about our people and services and the resources we offer such as our free online Privacy Library, please visit: http://www.mofo.com/privacy--data-security-services/ and "like" us on Facebook at http://www.facebook.com/MoFoPrivacy.

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.