Analysis of Proposed Consent Order to Aid Public Comment
In the Matter of Facebook, Inc., File No. 0923184

The Federal Trade Commission has accepted, subject to final approval, a consent agreement from Facebook, Inc. ("Facebook").

The proposed consent order has been placed on the public record for thirty (30) days for receipt of comments by interested persons. Comments received during this period will become part of the public record. After thirty (30) days, the Commission will again review the agreement and the comments received, and will decide whether it should withdraw from the agreement and take appropriate action or make final the agreement's proposed order.

Since at least 2004, Facebook has operated www.facebook.com, a social networking website that enables a consumer who uses the site ("user") to create an online profile and communicate with other users. Among other things, a user's online profile can include information such as the user's name, a "profile picture," interest groups they join, a "Friend List" of other users who are the user's "Friends" on the site, photo albums and videos they upload, and messages and comments posted by them or by other users. Users can also use third-party applications through the site ("Apps") to, for example, play games, take quizzes, track their physical fitness routines for comparison to their friends' routines, or receive discount offers or calendar reminders. As of August 2011, Facebook had more than 750 million users.

The Commission's complaint alleges eight violations of Section 5(a) of the FTC Act, which prohibits deceptive and unfair acts or practices in or affecting commerce, by Facebook:

- **Facebook's Deceptive Privacy Settings:** Facebook communicated to users that they could restrict certain information they provided on the site to a limited audience, such as "Friends Only." In fact, selecting these categories did not prevent users' information from being shared with Apps that their Friends used.

- **Facebook's Deceptive and Unfair December 2009 Privacy Changes:** In December 2009, Facebook changed its site so that certain information that users may have designated as private – such as a user's Friend List – was made public, without adequate disclosure to users. This conduct was also unfair to users.

- **Facebook's Deception Regarding App Access:** Facebook represented to users that whenever they authorized an App, the App would only access the information of the user that it needed to operate. In fact, the App could access nearly all of the user's information, even if unrelated to the App's operations. For example, an App that provided horoscopes for users could access the user's photos or employment information, even though there is no need for a horoscope App to access such information.

- **Facebook's Deception Regarding Sharing with Advertisers:** Facebook promised users that it would not share their personal information with advertisers; in fact, Facebook did share this information with advertisers when a user clicked on a Facebook ad.

- **Facebook's Deception Regarding its Verified Apps Program:** Facebook had a "Verified Apps" program through which it represented that it had certified the security of certain Apps when, in fact, it had not.

- **Facebook's Deception Regarding Photo and Video Deletion:** Facebook stated to users that, when they deactivate or delete their accounts, their photos and videos would be inaccessible. In fact, Facebook continued to allow access to this content even after a user deactivated or deleted his or her account.

- **Safe Harbor**: Facebook deceptively stated that it complied with the U.S.-EU Safe Harbor Framework, a mechanism by which U.S. companies may transfer data from the European Union to the United States consistent with European law.

The proposed order contains provisions designed to prevent Facebook from engaging in practices in the future that are the same or similar to those alleged in the complaint.

Part I of the proposed order prohibits Facebook from misrepresenting the privacy or security of "covered information," as well as the company's compliance with any privacy, security, or other compliance program, including but not limited to the U.S.-EU Safe Harbor Framework. "Covered information" is defined broadly as "information from or about an individual consumer, including but not limited to: (a) a first or last name; (b) a home or other physical address, including street name and name of city or town; (c) an email address or other online contact information, such as an instant messaging user identifier or a screen name; (d) a mobile or other telephone number; (e) photos and videos; (f) Internet Protocol ("IP") address, User ID, or other persistent identifier; (g) physical location; or (h) any information combined with any of (a) through (g) above."

Part II of the proposed order requires Facebook to give its users a clear and prominent notice and obtain their affirmative express consent before sharing their previously-collected information with third parties in any way that materially exceeds the restrictions imposed by their privacy settings. A "material . . . practice is one which is likely to affect a consumer's choice of or conduct regarding a product." FTC Policy Statement on Deception, Appended to *Cliffdale Associates, Inc*., 103 F.T.C. 110, 174 (1984).

Part III of the proposed order requires Facebook to implement procedures reasonably designed to ensure that a user's covered information cannot be accessed from Facebook's servers after a reasonable period of time, not to exceed thirty (30) days, following a user's deletion of his or her account.

Part IV of the proposed order requires Facebook to establish and maintain a comprehensive privacy program that is reasonably designed to: (1) address privacy risks related to the development and management of new and existing products and services, and (2) protect the privacy and confidentiality of covered information. The privacy program must be documented in writing and must contain controls and procedures appropriate to Facebook's size

and complexity, the nature and scope of its activities, and the sensitivity of covered information. Specifically, the order requires Facebook to:

- designate an employee or employees to coordinate and be responsible for the privacy program;
- identify reasonably-foreseeable, material risks, both internal and external, that could result in the unauthorized collection, use, or disclosure of covered information and assess the sufficiency of any safeguards in place to control these risks;
- design and implement reasonable controls and procedures to address the risks identified through the privacy risk assessment and regularly test or monitor the effectiveness of these controls and procedures;
- develop and use reasonable steps to select and retain service providers capable of appropriately protecting the privacy of covered information they receive from respondent, and require service providers by contract to implement and maintain appropriate privacy protections; and
- evaluate and adjust its privacy program in light of the results of the testing and monitoring, any material changes to its operations or business arrangements, or any other circumstances that it knows or has reason to know may have a material impact on the effectiveness of its privacy program.

Part V of the proposed order requires that Facebook obtain within 180 days, and every other year thereafter for twenty (20) years, an assessment and report from a qualified, objective, independent third-party professional, certifying, among other things, that it has in place a privacy program that provides protections that meet or exceed the protections required by Part IV of the proposed order; and its privacy controls are operating with sufficient effectiveness to provide reasonable assurance that the privacy of covered information is protected.

Parts VI through X of the proposed order are reporting and compliance provisions. Part VI requires that Facebook retain all "widely disseminated statements" that describe the extent to which respondent maintains and protects the privacy, security, and confidentiality of any covered information, along with all materials relied upon in making such statements, for a period of three (3) years. Part VI further requires Facebook to retain, for a period of six (6) months from the date received, all consumer complaints directed at Facebook, or forwarded to Facebook by a third party, that relate to the conduct prohibited by the proposed order, and any responses to such complaints. Part VI also requires Facebook to retain for a period of five (5) years from the date received, documents, prepared by or on behalf of Facebook, that contradict, qualify, or call into question its compliance with the proposed order. Part VI additionally requires Facebook to retain for a period of three (3) years, each materially different document relating to its attempt to obtain the affirmative express consent of users referred to in Part II, along with documents and information sufficient to show each user's consent and documents sufficient to demonstrate, on

an aggregate basis, the number of users for whom each such privacy setting was in effect at any time Facebook has attempted to obtain such consent. Finally, Part VI requires that Facebook retain all materials relied upon to prepare the third-party assessments for a period of three (3) years after the date that each assessment is prepared.

Part VII requires dissemination of the order now and in the future to principals, officers, directors, and managers, and to all current and future employees, agents, and representatives having supervisory responsibilities relating to the subject matter of the order. Part VIII ensures notification to the FTC of changes in corporate status. Part IX mandates that Facebook submit an initial compliance report to the FTC and make available to the FTC subsequent reports. Part X is a provision "sunsetting" the order after twenty (20) years, with certain exceptions.

The purpose of the analysis is to aid public comment on the proposed order. It is not intended to constitute an official interpretation of the complaint or proposed order, or to modify the proposed order's terms in any way.