Analysis of Proposed Consent Order to Aid Public Comment
In the Matter of Snapchat, Inc.,
File No. 132 3078

The Federal Trade Commission has accepted, subject to final approval, a consent order applicable to Snapchat, Inc. ("Snapchat").

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.

Snapchat provides a mobile application that allows consumers to send and receive photo and video messages known as "snaps." Both the iTunes App Store and the Google Play store list Snapchat among the top 15 free applications. As of September 2013, users transmitted more than 350 million snaps daily. Before sending a snap, the application requires the sender to designate a period of time that the recipient will be allowed to view the snap, up to ten seconds. Snapchat markets the application as an "ephemeral" messaging application, and claimed that once the timer expires, the snap "disappears forever." Snapchat represented, for a certain period, on its product description page on the iTunes App Store and Google Play and on the "FAQ" page on its website that snaps disappear when the timer expires. Snapchat further claimed that if a recipient took a screenshot of a snap, the sender would be notified. Snapchat also provides its users with a feature to find friends on the service, and prompts users during registration to enter their mobile telephone number in order to find friends.

Count 1 of the Commission's complaint alleges that Snapchat misrepresented that when sending a message though its application, the message would disappear forever after the user-set time period expires. Count 2 of the complaint alleges that Snapchat misrepresented that the sender will be notified if the recipient takes a screenshot of a snap. The complaint alleges that several methods exist by which a recipient can use tools outside of the application to save snaps, allowing the recipient to view them indefinitely. Additionally, the complaint alleges that widely publicized methods existed by which recipients could easily circumvent Snapchat's screenshot detection mechanism and capture a screenshot of a snap without the sender being notified.

Count 3 of the complaint alleges that Snapchat misrepresented in its privacy policy that it does not access location-specific information from consumers' mobile devices. Contrary to this representation, the complaint alleges that for a certain period, the Snapchat application on Android transmitted Wi-Fi based and cell-based location information from user's mobile devices to an analytics tracking provider.

Count 4 of the complaint alleges that Snapchat misrepresented, for a certain period, in its user interface that a user's mobile phone number was the only personal information that Snapchat collected in order to find the user's friends. Count 5 of the complaint alleges that Snapchat misrepresented in its privacy policy that it collected only the user's email, phone number, and Facebook ID for the purpose of finding friends. However, the complaint alleges that when the user

chose to find friends, Snapchat collected not only the user's phone number, but also, without informing the user, the names and phones numbers of all the contacts in the user's mobile device address book.

Finally, Count 6 of the complaint alleges that Snapchat misrepresented that it employed reasonable security measures in the design of its find friends feature. Specifically, the complaint alleges that for a certain period of time, Snapchat failed to verify that the phone number that an iOS user entered into the application did, in fact, belong to the mobile device being used by that individual. Due to this failure, an individual could create an account using a phone number that belonged to another consumer, enabling the individual to send and receive snaps associated with another consumer's phone number. Additionally, for a certain period, Snapchat allegedly failed to implement effective restrictions on the number of find friends requests that any one account could make. Further, Snapchat allegedly failed to implement any restrictions on serial and automated account creation. As a result of these security failures, in December 2013, attackers were able to use multiple accounts to send millions of find friends requests and compile a database of 4.6 million Snapchat usernames and the associated phone numbers.

The proposed order contains provisions designed to prevent Snapchat from engaging in the future in practices similar to those alleged in the complaint. Part I of the proposed order prohibits Snapchat from misrepresenting the extent to which Snapchat or its products or services protect the privacy, security, or confidentiality of covered information, including: (1) the extent to which a message is deleted after being viewed by the recipient; (2) the extent to which Snapchat or its products or services are capable of detecting or notifying the sender when a recipient has captured a screenshot of, or otherwise saved, a message; (3) the categories of covered information collected; or (4) the steps taken to protect against misuse or unauthorized disclosure of covered information.

Part II of the proposed order requires Snapchat 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 for consumers, and (2) protect the privacy and confidentiality of covered information, whether collected by Snapchat or input into, stored on, captured with, or accessed through a computer using Snapchat's products or services. The privacy program must contain privacy controls and procedures appropriate to Snapchat's size and complexity, the nature and scope of Snapchat's activities, and the sensitivity of the covered information. Specifically, the proposed order requires Snapchat to:

- designate an employee or employees to coordinate and be accountable for the privacy program;

- identify material internal and external risks that could result in Snapchat's unauthorized collection, use, or disclosure of covered information, and asses the sufficiency of any safeguards in place to control these risks;

- design and implement reasonable privacy controls and procedures to address the risks identified through the privacy risk assessment, and regularly test or monitor the effectiveness of the privacy controls, and procedures;

- develop and use reasonable steps to select and retain service providers capable of maintaining security practices consistent with the order, and require service providers by contract to implement and maintain appropriate safeguards; and

- evaluate and adjust its privacy program in light of the results of testing and monitoring, any material changes to operations or business arrangement, or any other circumstances that Snapchat knows or has reason to know may have a material impact on its privacy program.

Part III of the proposed order requires Snapchat to obtain within the first one hundred eighty (180) days after service of the order, and on a biennial basis thereafter for a period of twenty (20) years, an assessment and report from a qualified, objective, independent third-party professional, certifying, among other things, that: (1) it has in place a privacy program that provides protections that meet or exceed the protections required by Part II of the proposed order; and (2) its privacy program is operating with sufficient effectiveness to provide reasonable assurance to protect the privacy of covered information.

Parts IV through VIII of the proposed order are reporting and compliance provisions. Part IV requires Snapchat to retain documents relating to its compliance with the order. The order requires that all of the documents be retained for a five-year period. Part V requires dissemination of the order now and in the future to all current and future principals, officers, directors, and managers, and to persons with responsibilities relating to the subject matter of the order. Part VI ensures notification to the FTC of changes in corporate status. Part VII mandates that Snapchat submit a compliance report to the FTC within 60 days, and periodically thereafter as requested. Part VIII is a provision "sunsetting" the order after twenty (20) years, with certain exceptions.

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