132 3078

UNITED STATES OF AMERICA
FEDERAL TRADE COMMISSION

COMMISSIONERS: **Edith Ramirez, Chairwoman**
Julie Brill
Maureen K. Ohlhausen
Joshua D. Wright
Terrell McSweeny

In the Matter of	)	**DOCKET NO.**
Snapchat, Inc.,	)	
a corporation.	)	

COMPLAINT

The Federal Trade Commission, having reason to believe that Snapchat, Inc. ("respondent") has violated the provisions of the Federal Trade Commission Act, and it appearing to the Commission that this proceeding is in the public interest, alleges:

1. Respondent Snapchat, Inc. ("Snapchat"), the successor corporation to Toyopa Group LLC, is a Delaware corporation with its principal office or place of business at 63 Market Street, Venice, California 90291.

2. The acts and practices of respondent as alleged in this complaint have been in or affecting commerce, as "commerce" is defined in Section 4 of the Federal Trade Commission Act.

RESPONDENT'S BUSINESS PRACTICES

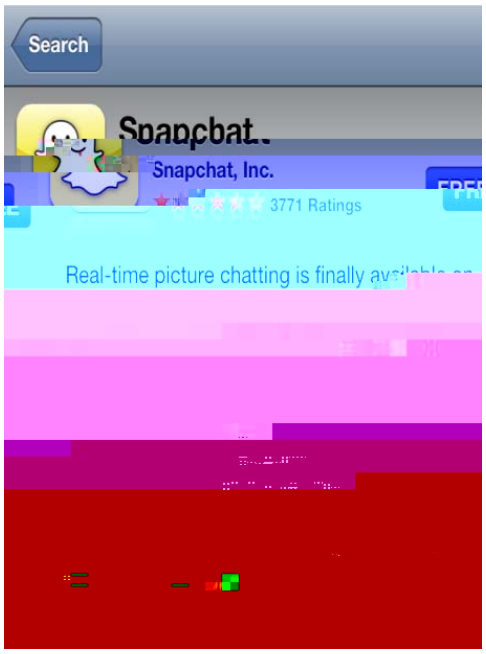
3. Snapchat provides a mobile application that allows consumers to send and receive photo and video messages known as "snaps." Before sending a snap, the application requires the sender to designate a period of time that the recipient will be allowed to view the snap. Snapchat markets the application as an "ephemeral" messaging application, having claimed that once the timer expires, the snap "disappears forever."

4. Snapchat launched its mobile application on Apple Inc.'s iOS operating system in September 2011 and on Google Inc.'s Android operating system in October 2012. Snapchat added video messaging to the iOS version of its application in December 2012 and to the Android version of its application in February 2013.

5. Both the iTunes App Store and the Google Play store list Snapchat among the top 15 free applications. As of September 2013, users transmit more than 350 million snaps daily.

SNAPCHAT'S "DISAPPEARING" MESSAGES
(Counts 1 and 2)

6. Snapchat marketed its application as a service for sending "disappearing" photo and video messages, declaring that the message sender "control[s] how long your friends can view your message." Before sending a snap, the application requires the sender to designate a period of time – with the default set to a maximum of 10 seconds – that the



8. From October 2012 to October 2013, Snapchat disseminated, or caused to be disseminated, to consumers the following statement on the "FAQ" page on its website:

> **Is there any way to view an image after the time has expired?**
> No, snaps disappear after the timer runs out. …

9. Despite these claims, several methods exist by which a recipient can use tools outside of the application to save both photo and video messages, allowing the recipient to access and view the photos or videos indefinitely.

10. For example, when a recipient receives a video message, the application stores the video file in a location outside of the application's "sandbox" (*i.e.*, the application's private storage area on the device that other applications cannot access). Because the file is stored in this unrestricted area, until October 2013, a recipient could connect his or her mobile device to a computer and use simple file browsing tools to locate and save the video file. This method for saving video files sent through the application was widely publicized as early as December 2012. Snapchat did not mitigate this flaw until October 2013, when it began encrypting video files sent through the application.

11. Furthermore, third-party developers have built applications that can connect to Snapchat's application programming interface ("API"), thereby allowing recipients to log into the Snapchat service without using the official Snapchat application. Because the timer and related "deletion" functionality is dependent on the recipient's use of the official Snapchat application, recipients can instead simply use a third-party application to download and save both photo and video messages. As early as June 2012, a security researcher warned Snapchat that it would be "pretty easy to write a tool to download and save the images a user receives" due to the way the API functions. Indeed, beginning in spring 2013, third-party developers released several applications on the iTunes App Store

and Google Play that recipients can use to save and view photo or video messages indefinitely. On Google Play alone, ten of these applications have been downloaded as many as 1.7 million times.

12. The file browsing tools and third-party applications described in paragraphs 10 and 11 are free or low cost and publicly available on the Internet. In order to download, install, and use these tools, a recipient need not make any modifications to the iOS or Android operating systems and would need little technical knowledge.

13. In addition to the methods described in paragraphs 10-12, a recipient can use the mobile device's screenshot capability to capture an image of a snap while it appears on the device screen.

14. Snapchat claimed that if a recipient took a screenshot of a snap, the sender would be notified. On its product description pages, as described in paragraph 7, Snapchat stated: "We'll let you know if [recipients] take a screenshot!" In addition, from October 2012 to February 2013, Snapchat disseminated, or caused to be disseminated, to consumers the following statement on the "FAQ" page on its website:

> **What if I take a screenshot?**
> Screenshots can be captured if you're quick. The sender will be notified immediately.

15. However, recipients can easily circumvent Snapchat's screenshot detection mechanism. For example, on versions of iOS prior to iOS 7, the recipient need only double press the device's Home button in rapid succession to evade the detection mechanism and take a screenshot of any snap without the sender being notified. This method was widely publicized.

Count 1

16. As described in Paragraphs 6, 7, and 8, Snapchat has represented, expressly or by implication, that when sending a message through its application, the message will disappear forever after the user-set time period expires.

17. In truth and in fact, as described in Paragraph 96 Tc-.0012 Tw[(shot-1.7bappear forever,Os p 12 0 0 1251

Users can also access this "Find Friends" feature at any time through the application's menu options.

26. However, when the user chooses to Find Friends, Snapchat collects not only the phone number a user enters, but also, without informing the user, the names and phone numbers of all the contacts in the user's mobile device address book.

27. Snapchat did not provide notice of, or receive user consent for, this collection until September 2012, at which time the iOS operating system was updated to provide a notification when an application accessed the user's address book.

Count 4

28. As described in Paragraphs 25, through its user interface, Snapchat represented, expressly or by implication, that the only personal information Snapchat collected when the user chose to Find Friends was the mobile number that the user entered.

29. In truth and in fact, as described in Paragraph 26, the mobile number that the user entered was not the only personal information that Snapchat collected. Snapchat also collected the names and phone numbers of all contacts in the user's mobile device address book. Therefore, the representation set forth in Paragraph 28 is false or misleading.

Snapchat's Deceptive Privacy Policy Statement Regarding the Find Friends Feature

30. From June 2011 to February 2013, Snapchat disseminated or caused to be disseminated to consumers the following statements, or similar statements, in its privacy policy regarding its Find Friends feature:

> Optional to the user, we also collect an email, phone number, and facebook id for purpose of finding friends on the serv

31. As explained in Paragraph 26, the Snapchat application collected more than email, phone number, and Facebook ID for purpose of finding friends on the service. The application collected the names and phone numbers of all contacts in the user's mobile device address book.

Count 5

32. As described in Paragraph 30, Snapchat, through its privacy policy, represented, expressly or by implication, that the only personal information Snapchat collected from a user for the purpose of finding friends on the service was email, phone number, and Facebook ID.

33. In truth and in fact, as described in Paragraph 31, email, phone number, and Facebook ID was not the only personal information that Snapchat collected for the purpose of finding friends on the service. Snapchat collected the names and phone numbers of all contacts in the user's mobile device address book when the user chose to Find Friends. Therefore, the representation set forth in Paragraph 32 is false or misleading.

SNAPCHAT'S FAILURE TO SECURE ITS FIND FRIENDS FEATURE (Count 6)

34. Snapchat failed to securely design its Find Friends feature. As described in paragraph 25, Snapchat prompts the user to enter a mobile phone number that will be associated with the user's account. In addition, as described in paragraph 26, Snapchat collects the names and phone numbers of all the contacts in the user's address book. Snapchat's API uses this information to locate the user's friends on the service.

35. From September 2011 to December 2012, 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.

36. Numerous consumers complained to Snapchat that individuals had created Snapchat accounts with phone numbers belonging to other consumers, leading to the misuse and unintentional disclosure of consumers' personal information. For example, consumers complained that they had sent snaps to accounts under the belief that they were communicating with a friend, when in fact they were not, resulting in the unintentional disclosure of photos containing personal information. In addition, consumers complained that accounts associated with their phone numbers had been used to send inappropriate or offensive snaps.

37. Snapchat could have prevented the misuse and unintentional disclosure of consumers' personal information by verifying phone numbers using common and readily available methods.

38. Indeed, in December 2012, Snapchat began performing short-message-service ("SMS") verification to confirm that the entered phone number did in fact belong to the mobile device being used by that individual.

39. In addition, from September 2011 to December 2013, Snapchat failed to implement effective restrictions on the number of Find Friend requests that any one account could make to its API. Furthermore, Snapchat failed to implement any restrictions on serial and automated account creation. As a result of these failures, in December 2013, attackers were able to use multiple accounts to send millions of Find Friend requests using randomly generated phone numbers. The attackers were able to compile a database of 4.6 million Snapchat usernames and the associated mobile phone numbers. The exposure of usernames and mobile phone numbers could lead to costly spam, phishing, and other unsolicited communications.

40. From June 2011 to May 2012, Snapchat disseminated or caused to be disseminated to consumers the following statement in its privacy policy:

> The Toyopa Group, LLC is dedicated to securing customer data and, to that end, employs the best security practices to keep your data protected.

41. From May 2012 to February 2013, Snapchat disseminated or caused to be disseminated to consumers the following statement in its privacy policy:

> Snapchat takes reasonable steps to help protect your personal information in an effort to prevent loss, misuse, and unauthorized access, disclosure, alteration, and destruction.

42. From February 2013 to the present, Snapchat disseminated or caused to be disseminated to consumers the following statement in its privacy policy:

> We take reasonable measures to help protect information about you from loss, theft, misuse and unauthorized access, disclosure, alteration and destruction.

Count 6

43. As described in Paragraphs 40-42, Snapchat has represented, expressly or by implication, that it employs reasonable security measures to protect personal information from misuse and unauthorized disclosure.

44. In truth and in fact, as described in Paragraphs 34-39, in many instances, Snapchat did not employ reasonable security measures to protect personal information from misuse and unauthorized disclosure. Therefore, the representation set forth in Paragraph 43 is false or misleading.