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."

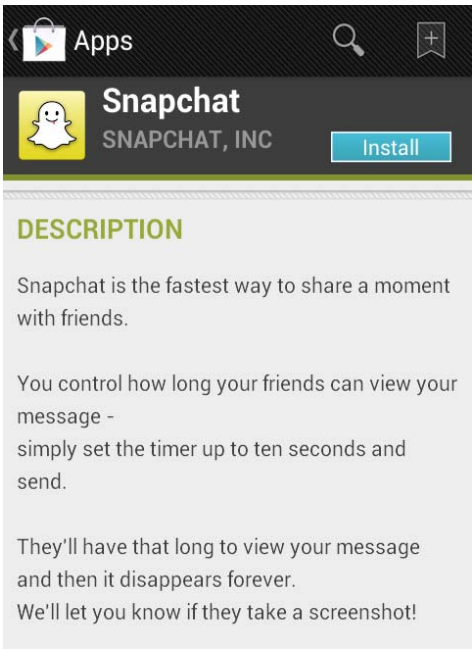
4. Snapchat launched its mobile application on Apple Inc.'s iOS operating system in September 2011 and on Google Inc.'s Android operating system in October 2012. Snapchat added video messaging to the iOS version of its application in December 2012 and to the Android version of its application in February 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 recipient will be allowed to view the snap, as depicted below:

7. Since the application's launch on iOS until May 2013, and since the application's launch on Android until June 2013, Snapchat disseminated, or caused to be disseminated, to consumers the following statements on its product description page on the iTunes App Store and Google Play:



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 9-12, when sending a message through its application, the message may not disappear forever after the user-set time period expires. Therefore, the representation set forth in Paragraph 16 is false or misleading.

Count 2

18. As described in Paragraphs 7 and 14, Snapchat has represented, expressly or by implication, that the sender will be notified if the recipient takes a screenshot of a snap.

19. In truth and in fact, as described in Paragraph 15, the sender may not be notified if the recipient takes a screenshot of a snap. Therefore, the representation set forth in Paragraph 18 is false or misleading.

SNAPCHAT'S COLLECTION OF GEOLOCATION INFORMATION (Count 3)

20. From June 2011 to February 2013, Snapchat disseminated or caused to be disseminated to consumers the following statements in its privacy policy:

> We do not ask for, track, or access any location-specific information from your device at any time while you are using the Snapchat application.

21. In October 2012, Snapchat integrated an analytics tracking service in the Android version of its application that acted as its service provider. While the Android operating system provided notice to consumers that the application may access location information, Snapchat did not disclose that it would, in fact, access location information, and continued to represent that Snapchat did "not ask for, track, or access any location-specific information . . ."

22. Contrary to the representation in Snapchat's privacy policy, from October 2012 to February 2013, the Snapchat application on Android transmitted Wi-Fi-based and cell-based location information from users' mobile devices to its analytics tracking service provider.

Count 3

23. As described in Paragraph 21, Snapchat has represented, expressly or by implication, that it does not collect users' location information.

24. In truth and in fact, as described in Paragraph 22, Snapchat did collect users' location information. Therefore, the representation set forth in Paragraph 23 is false or misleading.

SNAPCHAT'S COLLECTION OF CONTACTS INFORMATION (Counts 4 and 5)

Snapchat's Deceptive Find Friends User Interface

25. Snapchat provides its users with a feature to find friends on the service. During registration, the application prompts the user to "Enter your mobile number to find your friends on Snapchat!," implying – prior to September 2012 – through its user interface that the mobile phone number was the only information Snapchat collected to find the user's friends, as depicted below:

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 service. (Emphasis in original).

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.

45. The acts and practices of respondent as alleged in this complaint constitute deceptive acts or practices in or affecting commerce in violation of Section 5(a) of the Federal Trade Commission Act, 15 U.S.C. § 45(a).

THEREFORE, the Federal Trade Commission this ___ day of _____, 2014, has issued this complaint against respondent.

By the Commission.

Donald S. Clark
Secretary

UNITED STATES OF AMERICA
FEDERAL TRADE COMMISSION

In the Matter of	)	**AGREEMENT CONTAINING CONSENT ORDER**
Snapchat, Inc., a corporation.	)	**FILE NO. 132 3078**

The Federal Trade Commission ("Commission") has conducted an investigation of certain acts and practices of Snapchat, Inc. ("Snapchat" or "proposed respondent"). Proposed respondent, having been represented by counsel, is willing to enter into an agreement containing a consent order resolving the allegations contained in the attached draft complaint. Therefore,

IT IS HEREBY AGREED by and between Snapchat, Inc., by its duly authorized officers, and counsel for the Federal Trade Commission that:

1. Proposed respondent Snapchat, Inc., 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. Proposed respondent neither admits nor denies any of the allegations in the draft complaint, except as specifically stated in this order. Only for purposes of this action, proposed respondent admits the facts necessary to establish jurisdiction.

3. Proposed respondent waives:

   A. any further procedural steps;

   B. the requirement that the Commission's decision contain a statement of findings of fact and conclusions of law; and

   C. all rights to seek judicial review or otherwise to challenge or contest the validity of the order entered pursuant to this agreement.

4. This agreement shall not become part of the public record of the proceeding unless and until it is accepted by the Commission. If this agreement is accepted by the Commission, it, together with the draft complaint, will be placed on the public record for a period of thirty (30) days and information about it publicly released. The Commission thereafter may either withdraw its acceptance of this agreement and so notify proposed respondent, in which event it will take such action as it may consider appropriate, or issue and serve

its complaint (in such form as the circumstances may require) and decision in disposition of the proceeding.

5. This agreement is for settlement purposes only and does not constitute an admission by proposed respondent that the law has been violated as alleged in the draft complaint, or that the facts as alleged in the draft complaint, other than the jurisdictional facts, are true.

6. This agreement contemplates that, if it is accepted by the Commission, and if such acceptance is not subsequently withdrawn by the Commission pursuant to the provisions of Section 2.34 of the Commission's Rules, the Commission may, without further notice to proposed respondent, (1) issue its complaint corresponding in form and substance with the attached draft complaint and its decision containing the following order in disposition of the proceeding, and (2) make information about it public. When so entered, the order shall have the same force and effect and may be altered, modified, or set aside in the same manner and within the same time provided by statute for other orders. The order shall become final upon service. Delivery of the complaint and the decision and order to proposed respondent's address as stated in this agreement by any means specified in Section 4.4(a) of the Commission's Rules shall constitute service. Proposed respondent waives any right it may have to any other manner of service. The complaint may be used in construing the terms of the order. No agreement, understanding, representation, or interpretation not contained in the order or the agreement may be used to vary or contradict the terms of the order.

7. Proposed respondent has read the draft complaint and consent order. Proposed respondent understands that it may be liable for civil penalties in the amount provided by law and other appropriate relief for each violation of the order after it becomes final.

ORDER

DEFINITIONS

For purposes of this Order, the following definitions shall apply:

1. "Covered information" shall mean information from or about an individual consumer, including but not limited to (a) a first and 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 telephone number; (e) a persistent identifier, such as a customer number held in a "cookie," a static Internet Protocol ("IP") address, a mobile device ID, or processor serial number; (f) precise geo-location data of an individual or mobile device, including GPS-based, Wi-Fi-based, or cell-based location information; (g) an authentication credential, such as a username or password; or (h) any communications or content that is transmitted or stored through respondent's products or services.

2. "Computer" shall mean any desktop, laptop computer, tablet, handheld device, telephone, or other electronic product or device that has a platform on which to download, install, or run any software program, code, script, or other content and to play any digital audio, visual, or audiovisual content.

3. Unless otherwise specified, "respondent" shall mean Snapchat, Inc. and its successors and assigns.

4. "Commerce" shall mean as it is defined in Section 4 of the Federal Trade Commission Act, 15 U.S.C. § 44.

I.

IT IS ORDERED that respondent and its officers, agents, representatives, and employees, directly or indirectly, shall not misrepresent in any manner, expressly or by implication, in or affecting commerce, the extent to which respondent or its products or services maintain and protect the privacy, security, or confidentiality of any covered information, including but not limited to: (1) the extent to which a message is deleted after being viewed by the recipient; (2) the extent to which respondent 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.

II.

IT IS FURTHER ORDERED that respondent, in or affecting commerce, shall, no later than the date of service of this order, establish and implement, and thereafter 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 respondent or input into, stored on, captured with, or accessed through a computer using respondent's products or services. Such program, the content and implementation of which must be fully documented in writing, shall contain privacy controls and procedures appropriate to respondent's size and complexity, the nature and scope of respondent's activities, and the sensitivity of the covered information, including:

A. the designation of an employee or employees to coordinate and be accountable for the privacy program;

B. the identification of reasonably foreseeable, material risks, both internal and external, that could result in the respondent's unauthorized collection, use, or disclosure of covered information, and assessment of the sufficiency of any safeguards in place to control these risks. At a minimum, this privacy risk assessment should include consideration of risks in each area of relevant operation, including, but not limited to: (1) employee training and

management, including training on the requirements of this order; and (2) product design, development and research;

C. the design and implementation of reasonable privacy controls and procedures to address the risks identified through the privacy risk assessment, and regular testing or monitoring of the effectiveness of the privacy controls and procedures;

D. the development and use of reasonable steps to select and retain service providers capable of maintaining security practices consistent with this order, and requiring service providers by contract to implement and maintain appropriate safeguards;

E. the evaluation and adjustment of respondent's privacy program in light of the results of the testing and monitoring required by subpart C, any material changes to respondent's operations or business arrangements, or any other circumstances that respondent knows, or has reason to know, may have a material impact on the effectiveness of its privacy program.

III.

IT IS FURTHER ORDERED that, in connection with its compliance with Part II of this order, respondent shall obtain initial and biennial assessments and reports ("Assessments") from a qualified, objective, independent third-party professional, who uses procedures and standards generally accepted in the profession. A person qualified to prepare such Assessments shall have a minimum of three (3) years of experience in the field of privacy and data protection. All persons selected to conduct such assessments and prepare such reports shall be approved by the Associate Director for Enforcement, Bureau of Consumer Protection, Federal Trade Commission, 600 Pennsylvania Avenue, N.W., Washington, D.C. 20580. The reporting period for the Assessments shall cover: (1) the first one hundred eighty (180) days after service of the order for the initial Assessment; and (2) each two (2) year period thereafter for twenty (20) years after service of the order for the biennial Assessments. Each Assessment shall:

A. set forth the specific privacy controls that respondent has implemented and maintained during the reporting period;

B. explain how such privacy controls are appropriate to respondent's size and complexity, the nature and scope of respondent's activities, and the sensitivity of the covered information;

C. explain how the safeguards that have been implemented meet or exceed the protections required by Part II of this order; and

D. certify that the privacy controls are operating with sufficient effectiveness to provide reasonable assurance to protect the privacy of covered information and that the controls have so operated throughout the reporting period.

Each Assessment shall be prepared and completed within sixty (60) days after the end of the reporting period to which the Assessment applies. Respondent shall provide the initial Assessment to the Associate Director for Enforcement, Bureau of Consumer Protection, Federal Trade Commission, Washington, D.C. 20580, within ten (10) days after the Assessment has been prepared. All subsequent biennial Assessments shall be retained by respondent until the order is terminated and provided to the Associate Director of Enforcement within ten (10) days of request. Unless otherwise directed by a representative of the Commission, the initial Assessment, and any subsequent Assessments requested, shall be emailed to DEbrief@ftc.gov or sent by overnight courier (not the U.S. Postal Service) to: Associate Director for Enforcement, Bureau of Consumer Protection, Federal Trade Commission, 600 Pennsylvania Avenue NW, Washington, DC 20580 with the subject line *In the Matter of Snapchat, Inc.*, FTC File No. 1323078.

IV.

IT IS FURTHER ORDERED that respondent shall maintain and upon request make available to the Federal Trade Commission for inspection and copying, unless respondent asserts a valid legal privilege, a print or electronic copy of:

A. for a period of five (5) years from the date of preparation or dissemination, whichever is later, statements disseminated to consumers that describe the extent to which respondent maintains and protects the privacy, security and confidentiality of any covered information, including, but not limited to, any statement related to a change in any website or service controlled by respondent that relates to the privacy, security, and confidentiality of covered information, with all materials relied upon in making or disseminating such statements;

B. for a period of five (5) years from the date received, all consumer complaints directed at respondent, or forwarded to respondent by a third party, that relate to the conduct prohibited by this order and any responses to such complaints;

C. for a period of five (5) years from the date received, any documents, whether prepared by or on behalf of respondent that contradict, qualify, or call into question respondent's compliance with this order; and

D. for a period of five (5) years after the date of preparation of each Assessment required under Part III of this order, all materials relied upon to prepare the Assessment, whether prepared by or on behalf of respondent including but not limited to all plans, reports, studies, reviews, audits, audit trails, policies, training materials, and assessments, for the compliance period covered by such Assessment.

V.

IT IS FURTHER ORDERED that respondent shall deliver a copy of this order to all current and future subsidiaries, current and future principals, officers, directors, and managers, and to all current and future employees, agents, and representatives having responsibilities relating to the subject matter of this order. Respondent shall deliver this order to such current subsidiaries and personnel within thirty (30) days after service of this order, and to such future subsidiaries and personnel within thirty (30) days after the person assumes such position or responsibilities. For any business entity resulting from any change in structure set forth in Part VI, delivery shall be at least ten (10) days prior to the change in structure. Respondent must secure a signed and dated statement acknowledging receipt of this order, within thirty (30) days of delivery, from all persons receiving a copy of the order pursuant to this section.

VI.

IT IS FURTHER ORDERED that respondent shall notify the Commission at least thirty (30) days prior to any change in the corporation(s) that may affect compliance obligations arising under this order, including, but not limited to: a dissolution, assignment, sale, merger, or other action that would result in the emergence of a successor corporation; the creation or dissolution of a subsidiary, parent, or affiliate that engages in any acts or practices subject to this order; the proposed filing of a bankruptcy petition; or a change in the corporate name or address. Provided, however, that, with respect to any proposed change in the corporation(s) about which respondent learns fewer than thirty (30) days prior to the date such action is to take place, respondent shall notify the Commission as soon as is practicable after obtaining such knowledge. Unless otherwise directed by a representative of the Commission, all notices required by this Part shall be emailed to DEbrief@ftc.gov or sent by overnight courier (not the U.S. Postal Service) to: Associate Director for Enforcement, Bureau of Consumer Protection, Federal Trade Commission, 600 Pennsylvania Avenue NW, Washington, DC 20580 with the subject line *In the Matter of Snapchat, Inc.*, FTC File No. 1323078.

VII.

IT IS FURTHER ORDERED that respondent within ninety (90) days after the date of service of this order, shall file with the Commission a true and accurate report, in writing, setting forth in detail the manner and form of its compliance with this order. Within ten (10) days of receipt of written notice from a representative of the Commission, it shall submit an additional true and accurate written report.

VIII.

This order will terminate twenty (20) years from the date of its issuance, or twenty (20) years from the most recent date that the United States or the Commission files a complaint (with or without an accompanying consent decree) in federal court alleging any violation of the order, whichever comes later; provided, however, that the filing of such a complaint will not affect the duration of:

A. any Part in this order that terminates in fewer than twenty (20) years;

B. this order's application to any respondent that is not named as a defendant in such complaint; and

C. this order if such complaint is filed after the order has terminated pursuant to this Part.

Provided, further, that if such complaint is dismissed or a federal court rules that respondent did not violate any provision of the order, and the dismissal or ruling is either not appealed or upheld on appeal, then the order as to such respondent will terminate according to this Part as though the complaint had never been filed, except that the order will not terminate between the date such complaint is filed and the later of the deadline for appealing such dismissal or ruling and the date such dismissal or ruling is upheld on appeal.

Signed this _____ day of _____, 2014.

SNAPCHAT, INC.

Dated: _____ By: _____
EVAN SPIEGEL, Chief Executive Officer
Snapchat, Inc.

Dated: _____ By: _____
REBECCA S. ENGRAV, Esq.
Perkins Coie LLP
1201 Third Avenue, Suite 4900
Seattle, WA 98101

FEDERAL TRADE COMMISSION

Dated: _____ By: _____
ALLISON M. LEFRAK
Counsel for the Federal Trade Commission

_____
NITHAN SANNAPPA
Counsel for the Federal Trade Commission

APPROVED:

_____
CHRISTOPHER N. OLSEN
Assistant Director
Division of Privacy and Identity Protection

_____
MANEESHA MITHAL
Associate Director
Division of Privacy and Identity Protection

_____
JESSICA L. RICH
Director
Bureau of Consumer Protection