Analysis of Proposed Consent Order to Aid Public Comment
In the Matter of Uber Technologies, Inc., File No. 1523054

The Federal Trade Commission has accepted, subject to final approval, an agreement containing a consent order from Uber Technologies, Inc. ("Uber").

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 again will review the agreement and the comments received and will decide whether it should withdraw from the agreement or make final the agreement's proposed order.

Since 2010, Uber has operated a mobile application (the "App") that connects consumers who are transportation providers ("Drivers") with consumers seeking those services ("Riders"). Riders book transportation or delivery services through a publicly-available version of the App that can be downloaded to a smartphone. When a Rider requests transportation through the App, the request is conveyed to a nearby Uber Driver signed into the App.

Drivers are consumers who use the App to determine which ride requests they will accept. Uber collects a variety of personal information from Drivers, including names, email addresses, phone numbers, postal addresses, Social Security numbers, driver's license numbers, bank account information, vehicle registration information, and insurance information. With respect to Riders, Uber collects names, email addresses, postal addresses, and detailed trip records with precise geolocation information, among other things.

In November 2014, Uber was the subject of various news reports describing improper access and use of consumer personal information, including geolocation information, by Uber employees. One article reported that an Uber executive had suggested that Uber should hire "opposition researchers" to look into the "personal lives" of journalists who criticized Uber's practices. Another article described an aerial tracking tool known as "God View" that displayed the personal information of Riders using Uber's services. These reports led to considerable consumer uproar and calls by consumers to stop using Uber's services. In an effort to respond to consumer concerns, Uber issued a statement describing its policies concerning access to Rider and Driver data. As part of that statement, Uber promised that all "access to rider and driver accounts is being closely monitored and audited by data security specialists on an ongoing basis, and any violations of the policy will result in disciplinary action, including the possibility of termination and legal action."

As alleged in the proposed complaint, Uber has not monitored or audited its employees' access to Rider and Driver personal information on an ongoing basis since November 2014. In fact, between approximately August 2015 and May 2016, Uber did not timely follow up on automated alerts concerning the potential misuse of consumer personal information, and for approximately the first six months of this period only monitored access to account information

belonging to a set of internal high-profile users, such as Uber executives. During this time, Uber did not otherwise monitor internal access to personal information unless an employee specifically reported that a co-worker had engaged in improper access. The proposed complaint alleges that Uber's representation that it closely monitored and audited internal access to consumers' personal information was false or misleading in violation of Section 5 of the FTC Act in light of Uber's subsequent failure to monitor and audit such access between August 2015 and May 2016.

The proposed complaint also alleges that Uber failed to provide reasonable security for consumer information stored in a third-party cloud storage service provided by Amazon Web Services ("AWS") called the Amazon Simple Storage Service (the "Amazon S3 Datastore"). Uber stores a variety of files in the Amazon S3 Datastore that contain sensitive personal information, including full and partial back-ups of Uber databases. These back-ups contain a broad range of Rider and Driver personal information, including, among other things, names, email addresses, phone numbers, driver's license numbers and trip records with precise geolocation information.

From July 13, 2013 to July 15, 2015, Uber's privacy policy described the security measures Uber used to protect the personal information it collected from consumers, stating that such information "is securely stored within our databases, and we use standard, industry-wide commercially reasonable security practices such as encryption, firewalls and SSL (Secure Socket Layers) for protecting your information—such as any portions of your credit card number which we retain… and geo-location information." Additionally, Uber's customer service representatives offered assurances about the strength of Uber's security practices to consumers who were reluctant to submit personal information to Uber.

As described below, the proposed complaint alleges that the above statements violated Section 5 of the FTC Act because Uber engaged in a number of practices that, taken together, failed to provide reasonable security to prevent unauthorized access to Rider and Driver personal information in the Amazon S3 Datastore. Specifically, Uber allegedly:

- Until approximately September 2014, failed to implement reasonable access controls to safeguard data stored in the Amazon S3 Datastore. For example, Uber (1) permitted engineers to access the Amazon S3 Datastore with a single, shared AWS access key that provided full administrative privileges over all data stored there; (2) failed to restrict access to systems based on employees' job functions; and (3) failed to require multi-factor authentication for access to the Amazon S3 Datastore;

- Until approximately September 2014, failed to implement reasonable security training and guidance;

- Until approximately September 2014, failed to have a written information security program; and

- Until approximately March 2015, stored sensitive personal information in the Amazon S3 Datastore in clear, readable text, rather than encrypting the information.

As a result of these failures, on or about May 12, 2014, an intruder was able to gain access to Uber's Amazon S3 Datastore using an access key that one of Uber's engineers had posted to GitHub, a code-sharing site used by software developers. This key was publicly posted and granted full administrative privileges to all data and documents stored within Uber's Amazon S3 Datastore. The intruder accessed one file that contained sensitive personal information belonging to Uber Drivers, including over 100,000 unencrypted names and driver's license numbers, 215 unencrypted names and bank account and domestic routing numbers, and 84 unencrypted names and Social Security numbers. Uber did not discover the breach until September 2014, at which time Uber took steps to prevent further unauthorized access.

The proposed consent order contains provisions designed to prevent Uber from engaging in similar acts and practices in the future.

Part I of the proposed order prohibits Uber from making any misrepresentations about the extent to which Uber monitors or audits internal access to consumers' Personal Information or the extent to which Uber protects the privacy, confidentiality, security, or integrity of consumers' Personal Information.

Part II of the proposed order requires Uber to implement a mandated 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 consumers' personal information. Part III of the proposed order requires Uber to undergo biennial assessments of its mandated privacy program by a third party.

Parts IV through VIII of the proposed order are reporting and compliance provisions. Part IV requires dissemination of the order now and in the future to all current and future principals, officers, directors, and managers, and to persons with managerial or supervisory responsibilities relating to the subject matter of the order. Part V mandates that Uber submit a compliance report to the FTC one year after issuance of the order and submit additional notices as specified. Parts VI and VII require Uber to retain documents relating to its compliance with the order, and to provide such additional information or documents necessary for the Commission to monitor compliance. Part VIII states that the Order will remain in effect for 20 years.

The purpose of this 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 in any way the proposed order's terms.