Uber

Dear Uber EXT:

On October 25, 2018, Uber entered into a settlement agreement with the Federal Trade Commission, the regulatory agency responsible for U.S. consumer rights protections. The agreement will affect how Uber processes and protects U.S. user personal information.

Why this is important:
Earning and maintaining users' trust starts with honoring Uber's promises to them. This means that when we represent Uber to the public, we must be accurate about any claims we make about Uber's data privacy and data security practices, specifically about how Uber or we access, use, share, and protect user personal information. This affects statements Uber makes in advertisements, other marketing and promotional materials, blog posts, press interviews, presentations, and community operations communications to users.

It also affects Uber's and our practices internally because these practices must be consistent with any external claims Uber has made. In addition, Uber must engage in "privacy by design" and think about privacy risks and practices *before* engaging in any new data practices or changing its data practices.

How this affects you
Because you may have access to U.S. user personal information on behalf of Uber, you are required to receive and acknowledge a copy of the settlement agreement prior to beginning your role.

Acknowledged by:

Gyan Prakash
signature

GIYAN PRAKASH
printed name

02/23/2021
date

1523054

UNITED STATES OF AMERICA
BEFORE THE FEDERAL TRADE COMMISSION

COMMISSIONERS: Joseph J. Simons, Chairman
Noah Joshua Phillips
Rohit Chopra
Rebecca Kelly Slaughter
Christine S. Wilson

In the Matter of Uber Technologies, Inc., a corporation.	DECISION AND ORDER DOCKET NO. C-4662

DECISION

The Federal Trade Commission ("Commission") initiated an investigation of certain acts and practices of the Respondent named in the caption. The Commission's Bureau of Consumer Protection ("BCP") prepared and furnished to Respondent a draft Complaint. Respondent and BCP thereafter executed an Agreement Containing Consent Order ("Consent Agreement").

The Commission determined that it had reason to believe that Respondent had violated the Federal Trade Commission Act, and that a Complaint should issue stating its charges in that respect. The Commission accepted the executed Consent Agreement and placed it on the public record for a period of 30 days for the receipt and consideration of public comments. The Commission duly considered the comments received from interested persons pursuant to Commission Rule 2.34, 16 C.F.R. § 2.34, and the recommendations of its staff.

BCP then prepared and furnished to Respondent a revised draft Complaint that BCP proposed to present to the Commission for its consideration. Respondent and BCP executed a revised Consent Agreement containing (1) statements by Respondent that it neither admits nor denies any of the allegations in the Complaint, except as specifically stated in this Decision and Order, and that only for purposes of this action, it admits the facts necessary to establish jurisdiction; and (2) waivers and other provisions as required by the Commission's Rules.

The Commission thereafter reconsidered the matter and again determined that it had reason to believe that Respondent has violated the Federal Trade Commission Act, as stated in the revised Complaint, and that the revised Complaint should issue stating the Commission's charges in that respect. The Commission withdrew its acceptance of the original Consent Agreement and placed the revised Consent Agreement on the public record for a period of 30 days for the receipt and consideration of public comments. The Commission duly considered the comments received from interested persons pursuant to Commission Rule 2.34, 16 C.F.R. § 2.34, and the recommendations of its staff. Now, in further conformity with the procedures prescribed

in Commission Rule 2.34, the Commission issues its Complaint, makes the following Findings, and issues the following Order:

Findings

1. Respondent, Uber Technologies, Inc., is a Delaware corporation with its principal office or place of business at 1455 Market St. #400, San Francisco, California 94103.

2. The Commission has jurisdiction over the subject matter of this proceeding and over Respondent, and the proceeding is in the public interest.

ORDER

Definitions

For purposes of this Order, the following definitions apply:

A. "Covered Incident" means any instance in which any United States federal, state, or local law or regulation requires Respondent to notify any U.S. federal, state, or local government entity that information collected or received, directly or indirectly, by Respondent from or about an individual consumer was, or is reasonably believed to have been, accessed or acquired without authorization.

B. "Personal Information" means individually identifiable information collected or received, directly or indirectly, by Respondent from or about an individual consumer, including: (1) a first and last name; (2) a physical address; (3) an email address; (4) a telephone number; (5) a Social Security number; (6) a driver's license or other government-issued identification number; (7) a financial institution account number; (8) persistent identifiers associated with a particular consumer or device; or (9) precise geo-location data of an individual or mobile device, including GPS-based, WiFi-based, or cell-based location information.

C. "Respondent" means Uber Technologies, Inc. and its successors and assigns.

Provisions

I. Prohibition Against Misrepresentations

IT IS ORDERED that Respondent and Respondent's officers, agents, employees, and attorneys, and all other persons in active concert or participation with any of them, who receive actual notice of this Order, whether acting directly or indirectly, in connection with any product or service must not misrepresent in any manner, expressly or by implication:

A. the extent to which Respondent monitors or audits internal access to consumers' Personal Information; or

B. the extent to which Respondent protects the privacy, confidentiality, security, or integrity of any Personal Information.

II. Mandated Privacy Program

IT IS FURTHER ORDERED that Respondent must, no later than the effective date 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 Personal Information. Such program, the content and implementation of which must be documented in writing, must contain controls and procedures appropriate to Respondent's size and complexity, the nature and scope of Respondent's activities, and the sensitivity of the Personal Information, including:

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

B. the identification of reasonably foreseeable risks, both internal and external, that could result in Respondent's unauthorized collection, use, or disclosure of Personal Information and an assessment of the sufficiency of any safeguards in place to control these risks. At a minimum, this risk assessment should include consideration of risks in each area of relevant operation, including: (1) employee training and management, including training on the requirements of this Order; (2) product design, development, and research; (3) secure software design, development, and testing, including access key and secret key management and secure cloud storage; (4) review, assessment, and response to third-party security vulnerability reports, including through a "bug bounty" or similar program; and (5) prevention, detection, and response to attacks, intrusions, or systems failures;

C. the design and implementation of reasonable controls and procedures to address such risks and regular testing or monitoring of the effectiveness of those controls and procedures;

D. the development and use of reasonable steps to select and retain service providers capable of appropriately protecting the privacy of Personal Information they receive from Respondent and requiring service providers, by contract, to implement and maintain appropriate privacy protections for such Personal Information; and

E. the evaluation and adjustment of Respondent's privacy program in light of the results of the testing and monitoring required by sub-provision C, any changes to Respondent's operations or business arrangements, or any other circumstances that Respondent knows or has reason to know may have an impact on the effectiveness of the privacy program.

III. Privacy Assessments by a Third Party

IT IS FURTHER ORDERED that, in connection with its compliance with the Provision of this Order titled Mandated Privacy Program, Respondent must obtain initial and biennial assessments ("Assessments"):

A. The Assessments must be completed by a qualified, objective, independent third-party professional, who uses procedures and standards generally accepted in the profession. An individual qualified to prepare such Assessments must have a minimum of 3 years of

experience in the field of privacy and data protection. All individuals selected to complete such Assessments must be approved by the Associate Director for Enforcement, Bureau of Consumer Protection, Federal Trade Commission, in his or her sole discretion. Any decision not to approve an individual selected to conduct such Assessments must be accompanied by a writing setting forth in detail the reasons for denying such approval.

B. The reporting period for the Assessments must cover: (1) the first 180 days after the issuance date of the Order for the initial Assessment, and (2) each 2-year period thereafter for 20 years after the issuance date of the Order for the biennial Assessments.

C. Each Assessment must:

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

2. 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 Personal Information;

3. explain how the privacy controls that have been implemented meet or exceed the protections required by the Provision of this Order titled Mandated Privacy Program; and

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

D. Each Assessment must be completed within 60 days after the end of the reporting period to which the Assessment applies. Respondent must provide each Assessment to the Commission within 10 days after the Assessment has been completed. Respondent must notify the Commission of any portions of the Assessment containing trade secrets, commercial or financial information, or information about a consumer or other third party, for which confidential treatment is requested pursuant to the Commission's procedures concerning public disclosure set forth in 15 U.S.C. § 46(f) and 16 C.F.R. § 4.10.

IV. Covered Incident Reports

IT IS FURTHER ORDERED that Respondent, within a reasonable time after the date of Respondent's discovery of a Covered Incident, but in any event no later than 10 days after the date Respondent first notifies any U.S. federal, state, or local government entity of the Covered Incident, must submit a report to the Commission:

A. The report must include, to the extent possible:

1. the date, estimated date, or estimated date range when the Covered Incident occurred;

2. a description of the facts relating to the Covered Incident, including the causes and scope of the Covered Incident, if known;

3. a description of each type of information that triggered the notification obligation to the U.S. federal, state, or local government entity;

4. the number of consumers whose information triggered the notification obligation to the U.S. federal, state, or local government entity;

5. the acts that Respondent has taken to date to remediate the Covered Incident and protect Personal Information from further exposure or access; and

6. a representative copy of each materially different notice required by U.S. federal, state, or local law or regulation and sent by Respondent to consumers or to any U.S. federal, state, or local government entity.

B. Unless otherwise directed by a Commission representative in writing, all Covered Incident reports to the Commission pursuant to this Order must 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. The subject line must begin, "In re: Uber Technologies, Inc., File No. 1523054."

V. Acknowledgments of the Order

IT IS FURTHER ORDERED that Respondent obtain acknowledgments of receipt of this Order:

A. Respondent, within 10 days after the effective date of this Order, must submit to the Commission an acknowledgment of receipt of this Order sworn under penalty of perjury.

B. For 20 years after the issuance date of this Order, Respondent must deliver, or for contingent workers, cause to be delivered, a copy of this Order to (1) all principals, officers, directors, and LLC managers and members; (2) all employees, agents, and representatives who participate in conduct related to the subject matter of the Order, including all employees, agents, and representatives who regularly access Personal Information; and (3) any business entity resulting from any change in structure as set forth in the Provision of this Order titled Compliance Report and Notices. Delivery must occur within 10 days after the effective date of this Order for current personnel. For all others, delivery must occur before they assume their responsibilities.

C. From each individual or entity to which Respondent delivered, or caused to be delivered, a copy of this Order, Respondent must obtain, within 30 days, a signed and dated acknowledgment of receipt of this Order.

VI. Compliance Report and Notices

IT IS FURTHER ORDERED that Respondent make timely submissions to the Commission:

A. One year after the issuance date of this Order, Respondent must submit a compliance report, sworn under penalty of perjury, in which:

1. Respondent must: (a) identify the primary physical, postal, and email address and telephone number, as designated points of contact, that representatives of the Commission may use to communicate with Respondent; (b) identify all of Respondent's subsidiaries that are registered as business entities in any state of the United States by all of their names, primary telephone numbers, and physical, postal, email, and Internet addresses; (c) describe the activities of each business, including the products and services offered by each business and the Personal Information each business collects, maintains, transfers or stores; (d) describe in detail whether and how Respondent is in compliance with each Provision of this Order, including a discussion of all of the changes Respondent made to comply with the Order; and (e) provide a copy of each Acknowledgment of the Order obtained pursuant to this Order, unless previously submitted to the Commission.

B. Respondent must submit a compliance notice, sworn under penalty of perjury, within 14 days of any change in the following: (1) any designated point of contact; or (2) the structure of Respondent or any entity that Respondent has any ownership interest in or controls directly or indirectly that may affect compliance obligations arising under this Order, including: creation, merger, sale, or dissolution of the entity or any subsidiary, parent, or affiliate that engages in any acts or practices subject to this Order.

C. Respondent must submit notice of the filing of any bankruptcy petition, insolvency proceeding, or similar proceeding by or against Respondent within 14 days of its filing.

D. Any submission to the Commission required by this Order to be sworn under penalty of perjury must be true and accurate and comply with 28 U.S.C. § 1746, such as by concluding: "I declare under penalty of perjury under the laws of the United States of America that the foregoing is true and correct. Executed on: _____" and supplying the date, signatory's full name, title (if applicable), and signature.

E. Unless otherwise directed by a Commission representative in writing, all submissions to the Commission pursuant to this Order must 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. The subject line must begin: "In re: Uber Technologies, Inc., File No. 1523054."

VII. Recordkeeping

IT IS FURTHER ORDERED that Respondent must create certain records for 20 years after the issuance date of the Order, and retain each such record for 5 years, unless otherwise specified below. Specifically, Respondent must create and retain the following records:

A. Accounting records showing the revenues from all goods or services sold;

B. Personnel records showing, for each person providing services in relation to any aspect of the Order, whether as an independent contractor, employee or otherwise, that person's: name; addresses; telephone numbers; job title or position; dates of service; and (if applicable) the reason for termination;

C. Records of all consumer complaints directed at Respondent, or forwarded to Respondent by a third party, concerning the subject matter of the Order, and any response;

D. All records necessary to demonstrate full compliance with each Provision of this Order, including all submissions to the Commission;

E. A copy of each widely disseminated representation by Respondent that describes the extent to which Respondent maintains or protects the privacy, security, and confidentiality of Personal Information, including any representation concerning a change in Respondent's practices with respect to the privacy, security, and confidentiality of Personal Information;

F. For 5 years after the date of preparation of each Assessment required by this Order, all materials relied upon to prepare the Assessment, whether prepared by or on behalf of Respondent, including all plans, reports, studies, reviews, audits, audit trails, policies, training materials, and assessments, and any other materials concerning Respondent's compliance with related Provisions of this Order, for the compliance period covered by such Assessment;

G. For 5 years from the date created or received, reports received by Respondent from individuals or entities that seek payment, rewards, or recognition through a "bug bounty" or similar program for reporting a security vulnerability that relates to potential or actual access to or acquisition of Personal Information, and records sufficient to show Respondent's review, assessment of, and response to any such reports;

H. For 5 years from the date created or received, copies of all subpoenas and other communications with law enforcement, if such communications relate to Respondent's compliance with this Order; and

I. For 5 years from the date created or received, all records, whether prepared by or on behalf of Respondent, that contradict, qualify, or call into question Respondent's compliance with this Order.

VIII. Compliance Monitoring

IT IS FURTHER ORDERED that, for the purpose of monitoring Respondent's compliance with this Order:

A. Within 10 days of receipt of a written request from a representative of the Commission, Respondent must: submit additional compliance reports or other requested information, which must be sworn under penalty of perjury, and produce records for inspection and copying.

B. For matters concerning this Order, representatives of the Commission are authorized to communicate directly with Respondent. Respondent must permit representatives of the Commission to interview anyone affiliated with Respondent who has agreed to such an interview. The interviewee may have counsel present.

C. The Commission may use all other lawful means, including posing through its representatives as consumers, suppliers, or other individuals or entities, to Respondent or any individual or entity affiliated with Respondent, without the necessity of identification or prior notice. Nothing in this Order limits the Commission's lawful use of compulsory process, pursuant to Sections 9 and 20 of the FTC Act, 15 U.S.C. §§ 49, 57b-1.

IX. Order Effective Dates

IT IS FURTHER ORDERED that this Order is final and effective upon the date of its publication on the Commission's website (ftc.gov) as a final order. This Order will terminate on October 25, 2038, or 20 years from the most recent date that the United States or the Commission files a complaint (with or without an accompanying settlement) in federal court alleging any violation of this Order, whichever comes later; *provided, however*, that the filing of such a complaint will not affect the duration of:

A. Any Provision in this Order that terminates in less than 20 years;

B. This Order's application to a 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 Provision.

Provided, further, that if such complaint is dismissed or a federal court rules that the 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 will terminate according to this Provision 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.

By the Commission, Commissioner Wilson not participating.

Donald S. Clark
Secretary

SEAL:
ISSUED: October 25, 2018