

Complaint

IN THE MATTER OF

UBER TECHNOLOGIES, INC.CONSENT ORDER, ETC. IN REGARD TO ALLEGED VIOLATIONS OF SECTION 5 OF THE FEDERAL
TRADE COMMISSION ACT*Docket No. C-4662; File No. 152 3054**Complaint, October 25, 2018 – Decision, October 25, 2018*

This consent order addresses Uber Technologies, Inc.’s access and use of consumer personal information, including geolocation information. The complaint alleges that Uber has not monitored or audited its employees’ access to Rider and Driver personal information on an ongoing basis since November 2014. The complaint also alleges that Uber failed to provide reasonable security for consumer information stored in a third-party cloud storage service. The consent 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. The Order also 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.

Participants

For the *Commission*: Ben Rossen and James A. Trilling.

For the *Respondent*: Erin Earl, Rebecca Engrav and Janis Kestenbaum, Perkins Coie LLP.

COMPLAINT

The Federal Trade Commission (“Commission”), having reason to believe that Uber Technologies, Inc. (“Respondent” or “Uber”), a corporation, has violated the Federal Trade Commission Act, 15 U.S.C. § 45(a), and it appearing to the Commission that this proceeding is in the public interest, alleges:

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

2. The acts and practices of Respondent 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. Since at least 2010, Respondent has distributed a mobile software application (the “App”) that connects consumers who are transportation providers (hereinafter “Uber Drivers” or “Drivers”) with consumers seeking those services (hereinafter “Riders”). Respondent markets

Complaint

different versions of the App to Riders and Drivers. Respondent also operates a website at www.uber.com.

4. Riders book transportation services from an Uber Driver using 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.

5. Uber Drivers are consumers who use the App to locate Riders in need of transportation. Respondent recruits and approves consumers to become Uber Drivers, sets the rates that Drivers charge for providing transportation, and collects a portion of the fares that Drivers charge for each ride. Drivers decide when they are available to accept ride requests and use the App to determine which ride requests they will accept.

6. When a consumer signs up to become an Uber Driver, Respondent collects personal information about the consumer, including the consumer's name, email address, phone number, postal address, profile picture, Social Security number, driver's license information, bank account information (including domestic routing and bank account numbers), vehicle registration information, and insurance information.

7. Respondent also collects and stores a variety of personal information from Riders, including, among other things, names, email addresses, postal addresses, profile pictures, and detailed trip records including precise geolocation information.

8. Respondent collects precise geolocation information about both Riders and Drivers in real time. When a Rider requests transportation services and has authorized Respondent to collect such information, Respondent collects precise geolocation information from the Rider's device. During a trip, Respondent collects precise geolocation information from the Rider's device if the Rider has provided consent for Respondent to do so. Respondent also collects such information about the route of the trip from the Driver's mobile device and associates the trip information with the Rider.

9. As of December 2014, there were more than 160,000 active Uber Drivers using the App. As of December 2015, Riders had completed more than 1 billion rides using Respondent's services. In 2015, Respondent had over \$1.5 billion in total revenues.

RESPONDENT'S INTERNAL ACCESS TO CONSUMER PERSONAL INFORMATION

10. In November 2014, Respondent was the subject of a number of widely disseminated news reports concerning allegations of improper access and use of consumer personal information, including geolocation data. One article, published on November 17, 2014, reported that an Uber executive had suggested Respondent should hire "opposition researchers" and journalists to look into the "personal lives" of journalists who criticized Respondent's business practices. On November 18, 2014, another article described an internal aerial tracking tool, referred to as "God View," that displayed the personal information of Riders using

Complaint

Respondent's services. These reports were widely circulated in the press and caused considerable consumer uproar.

11. In an effort to respond to consumer concerns, on November 18, 2014, Respondent issued a statement, which has been continuously posted on Respondent's website and was widely disseminated in the press, describing Respondent's policies concerning access to Rider and Driver data. Respondent stated:

Uber has a strict policy prohibiting all employees at every level from accessing a rider or driver's data. The only exception to this policy is for a limited set of legitimate business purposes. Our policy has been communicated to all employees and contractors....

The policy is also clear that 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.

(Exhibit A.)

12. Despite Respondent's representation that its practices would continue on an ongoing basis, Respondent has not always closely monitored and audited its employees' access to Rider and Driver accounts since November 2014. Respondent developed an automated system for monitoring employee access to consumer personal information in December 2014 but the system was not designed or staffed to effectively handle ongoing review of access to data by Respondent's thousands of employees and contingent workers.

13. In approximately August 2015, Respondent ceased using the automated system it had developed in December 2014 and began to develop a new automated monitoring system. From approximately August 2015 until May 2016, Respondent 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, Respondent only monitored access to account information belonging to a set of internal high-profile users, such as Uber executives. During this time, Respondent did not otherwise monitor internal access to personal information unless an employee specifically reported that a co-worker had engaged in inappropriate access.

RESPONDENT'S AMAZON S3 DATASTORE

14. As part of its information technology infrastructure, Respondent uses a third-party service provided by Amazon Web Services ("AWS") called the Amazon Simple Storage Service (the "Amazon S3 Datastore"). The Amazon S3 Datastore is a scalable cloud storage service that can be used to store and retrieve large amounts of data. The Amazon S3 Datastore stores data inside of virtual containers, called "buckets," against which individual access controls can be applied.

Complaint

15. Respondent relies on the Amazon S3 Datastore to store a wide variety of files that contain sensitive personal information. These files include, among other things, full and partial back-ups of Uber databases. The database back-ups contain a broad range of Rider and Driver personal information, including, among other things, names, nicknames, email addresses, postal addresses, phone numbers, unique device identifiers, trip records, geolocation information, and driver's license numbers. The files also include documents provided by Uber Drivers, such as vehicle registration receipts, proof of insurance documents, and images of driver's licenses.

RESPONDENT'S SECURITY STATEMENTS

16. From at least July 13, 2013 to July 15, 2015, Respondent disseminated, or caused to be disseminated, a privacy policy that expressly applied to Respondent's websites and Apps and contained the following statements regarding the security measures Respondent used to protect the personal information it collected from consumers:

The Personal Information and Usage Information we collect 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 (we do not ourselves retain your entire credit card information) and geo-location information.

(Exhibit B.)

17. In numerous instances, Respondent's customer service representatives offered assurances about the strength of Respondent's security practices to consumers who were reluctant to submit personal information to Uber, including but not limited to the following:

“Your information will be stored safely and used only for purposes you've authorized. **We use the most up to date technology and services to ensure that none of these are compromised.**”

“I understand that you do not feel comfortable sending your personal information via online. However, **we're extra vigilant in protecting all private and personal information.**”

“All of your personal information, including payment methods, is **kept secure and encrypted to the highest security standards available.**”

(Emphases added.)

Complaint

RESPONDENT'S SECURITY PRACTICES

18. Respondent has engaged in a number of practices that, taken together, failed to provide reasonable security to prevent unauthorized access to Rider and Driver personal information stored in the Amazon S3 Datastore. Among other things, Respondent:

- a. Failed to implement reasonable access controls to safeguard data stored in the Amazon S3 Datastore. For example, Respondent:
 - i. until approximately September 2014, failed to require programs and engineers that access the Amazon S3 Datastore to use distinct access keys, instead permitting all programs and engineers to use a single AWS access key that provided full administrative privileges over all data in the Amazon S3 Datastore;
 - ii. until approximately September 2014, failed to restrict access to systems based on employees' job functions; and
 - iii. until approximately September 2015, failed to require multi-factor authentication for individual account access, and until at least November 2016, failed to require multi-factor authentication for programmatic service account access, to the Amazon S3 Datastore;
- b. Until at least September 2014, failed to implement reasonable security training and guidance;
- c. Until approximately September 2014, failed to have a written information security program; and
- d. Until at least November 2016, stored sensitive personal information in the Amazon S3 Datastore in clear, readable text, including in database backups and database prune files, rather than encrypting the information.

19. Respondent could have prevented or mitigated the failures described in **Paragraph 18** through relatively low-cost measures.

20. Respondent's failure to provide reasonable security for consumers' personal information stored in its databases, including geolocation information, created serious risks for consumers.

2014 DATA BREACH

21. As a result of the failures described in **Paragraph 18**, on or about May 12, 2014, an intruder was able to access consumers' personal information in plain text in Respondent's Amazon S3 Datastore using an access key that one of Respondent's engineers had publicly posted to GitHub, a code-sharing website used by software developers. The publicly posted key

Complaint

granted full administrative privileges to all data and documents stored within Respondent'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. The file also contained other Uber Driver information, including physical addresses, email addresses, mobile device phone numbers, device IDs, and location information from trips the Uber Drivers provided.

22. Respondent did not discover the existence of the breach until September 2014.

23. Respondent initially sent breach notification letters to 48,949 affected Uber Drivers in February 2015. In May and July of 2016, Uber learned of more individuals affected by the breach, including approximately 60,000 additional Uber Drivers whose unencrypted names and driver's license numbers were accessed. Uber sent additional breach notification letters to these affected Uber Drivers in June and August of 2016.

2016 DATA BREACH

24. On or about November 14, 2016, Respondent learned of another breach of consumer personal information stored in Uber's Amazon S3 Datastore. Once again, intruders gained access to the Amazon S3 Datastore using an access key that an Uber engineer had posted to GitHub. This time, the key was in plain text in code that was posted to a private GitHub repository. However, Uber granted its engineers access to Uber's GitHub repositories through engineers' individual GitHub accounts, which engineers generally accessed through personal email addresses. Uber did not have a policy prohibiting engineers from reusing credentials, and did not require engineers to enable multi-factor authentication when accessing Uber's GitHub repositories. The intruders said that they accessed Uber's GitHub page using passwords that were previously exposed in other large data breaches, whereupon they discovered the access key in plain text. The intruders downloaded 16 files from Respondent's Amazon S3 Datastore between October 13, 2016 and November 15, 2016. These files contained unencrypted consumer personal information relating to U.S. Riders and Drivers, including, among other things, approximately 25.6 million names and email addresses, 22.1 million names and mobile phone numbers, and 607,000 names and driver's license numbers. Nearly all of the exposed personal information was collected before July 2015 and stored in unencrypted database backup files.

25. Respondent discovered the breach on or about November 14, 2016, when one of the attackers contacted Respondent claiming to have compromised Uber's "databases" and demanding a six-figure payout.

26. Respondent paid the attackers \$100,000 through the third party that administers Uber's "bug bounty" program. Respondent created the bug bounty program to pay financial rewards in exchange for the responsible disclosure of serious security vulnerabilities. However, the attackers in this instance were fundamentally different from legitimate bug bounty recipients. These attackers did not merely identify a vulnerability and disclose it responsibly. Rather, the

Complaint

attackers maliciously exploited the vulnerability and acquired personal information relating to millions of consumers.

27. Respondent failed to disclose the breach to affected consumers until November 21, 2017, more than a year after discovery of the breach. Furthermore, the November 2016 breach occurred in the midst of a nonpublic investigation by the Commission relating to Respondent's data security practices, including, specifically, the security of Respondent's Amazon S3 Datastore. Despite the pendency of this investigation, Respondent failed to disclose the existence of the breach to the Commission until November 2017.

COUNT 1

28. As described in **Paragraph 11**, Respondent has represented, directly or indirectly, expressly or by implication, that internal access to consumers' personal information is closely monitored and audited by data security specialists on an ongoing basis.

29. In truth and in fact, as described in **Paragraphs 12 - 13**, Respondent has not closely monitored and audited internal access to consumers' personal information by data security specialists on an ongoing basis. Therefore, the representation set forth in **Paragraph 28** is false or misleading.

COUNT 2

30. As described in **Paragraphs 16 - 17**, Respondent has represented, directly or indirectly, expressly or by implication, that it would provide reasonable security for consumers' personal information stored in its databases.

31. In truth and in fact, as described in **Paragraphs 18 - 27**, Respondent did not provide reasonable security for consumers' personal information stored in its databases. Therefore, the representation set forth in **Paragraph 30** is false or misleading.

32. The acts and practices of Respondent as alleged in this Complaint constitute unfair or 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 twenty-fifth day of October, 2018, has issued this Complaint against Respondent.

By the Commission, Commissioner Wilson not participating.

Complaint

Exhibit A

Uber's Data Privacy Policy

<https://newsroom.uber.com/ubers-data-privacy-policy/>

Uber's Data Privacy Policy

November 18, 2014 Posted by Nairi

We wanted to take a moment to make very clear our policy on data privacy, which is fundamental to our commitment to both riders and drivers. Uber has a strict policy prohibiting all employees at every level from accessing a rider or driver's data. The only exception to this policy is for a limited set of legitimate business purposes. Our policy has been communicated to all employees and contractors.

Examples of legitimate business purposes for select members of the team include:

- Supporting riders and drivers in order to solve problems brought to their attention by the Uber community.
- Facilitating payment transactions for drivers.
- Monitoring driver and rider accounts for fraudulent activity, including terminating fake accounts and following up on stolen credit card reports.
- Reviewing specific rider or driver accounts in order to troubleshoot bugs.

The policy is also clear that 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.

Uber's business depends on the trust of the riders and

Destinations

Sign up to ride or drive
Driver Stories



Impact

Inside Uber

RIDE >



DRIVE >

Complaint

[Uber's Data Privacy Policy](#)<https://newsroom.uber.com/ubers-data-privacy-policy/>

drivers that use our technology and platform. The trip history of our riders is confidential information, and Uber protects this data from internal and external unauthorized access. As the company continues to grow, we will continue to be transparent about our policy and ensure that it is properly understood by our employees.

Complaint

Exhibit B

Uber - Legal

<https://web.archive.org/web/20141018005925/https://www.uber.com/legal...>

LEGAL

[USER TER...](#) [PRIVACY P...](#) [COPYRIGH...](#) [SECURITY ...](#) [OTHER \(W...](#)

UBER PRIVACY POLICY

GLOBAL ▼

effective July 13, 2013

Your privacy matters to Uber Technologies, Inc. (the "Company", "we", or "us"). This Privacy Policy explains how we collect, use, share and protect information about you. We also provide information regarding how you can access and update your information and make certain choices about how your information is used.

The Privacy Policy covers both our "online" (e.g., web and mobile services, including any web sites operated by us such as [www.uber.com \(/web/20141018005925/https://www.uber.com/\)](https://www.uber.com/), [m.uber.com \(/web/20141018005925/https://m.uber.com/\)](https://m.uber.com/), mobile applications, however accessed and/or used, whether via personal computers, mobile devices or otherwise) and "offline" (e.g., collection of data through mailings, telephone, or in person) activities owned, operated, provided, or made available by the Company. Our "online" and "offline" activities are collectively referenced as the "**Services**." This Privacy Policy also applies to

Complaint

Uber - Legal

<https://web.archive.org/web/20141018005925/https://www.uber.com/legal...>

your use of interactive features or downloads that: (i) we own or control; (ii) are available through the Services; or (iii) interact with the Services and post or incorporate this Privacy Policy.

BY USING OUR SERVICES OR BY OTHERWISE GIVING US YOUR INFORMATION, YOU AGREE TO THE TERMS OF THIS PRIVACY POLICY. Please review the following carefully so that you understand our privacy practices. If you do not agree to this Privacy Policy, do not use any of our Services or give us any of your information. In addition, please review our Terms and Conditions ([/web/20141018005925/https://www.uber.com/legal/terms](https://web/20141018005925/https://www.uber.com/legal/terms)), which may apply to your use of our websites and mobile applications. This Privacy Policy is incorporated by reference into the applicable Terms and Conditions.

If you have questions about this Privacy Policy, please contact us at privacy@uber.com. (<mailto:privacy@uber.com>)

Uber Technologies, Inc. complies with the U.S. – E.U. Safe Harbor framework and the U.S. - Swiss Safe Harbor framework as set forth by the U.S. Department of Commerce regarding the collection, use, and retention of personal data from European Union member countries and Switzerland. Uber Technologies, Inc. has certified that it adheres to the Safe Harbor Privacy Principles of notice, choice, onward transfer, security, data integrity, access, and enforcement. To learn more about the Safe Harbor program, and to view Uber Technologies, Inc.'s certification, please visit <http://www.export.gov/safeharbor/> ([/web/20141018005925/http://www.export.gov/safeharbor/](https://web/20141018005925/http://www.export.gov/safeharbor/)).

TABLE OF CONTENTS

1. What Information Do We Collect?
 - a. Information You Provide To Us
 - b. Information We Collect As You Access And Use Our Services
 - c. Information Third Parties Provide About You
 - d. Information You Provide About A Third Party
 - e. Information Collected by Mobile Applications

Complaint

Uber - Legal

<https://web.archive.org/web/20141018005925/https://www.uber.com/legal...>

2. How Do We Use The Information Collected?

3. How and When Do We Disclose Information To Third Parties?

- a. When You Agree To Receive Information From Third Parties
- b. Third Parties Providing Services on Our Behalf
- c. Co-branded Areas
- d. Sweepstakes, Contests And Promotions
- e. Administrative and Legal Reasons
- f. Business Transfer

4. What is Online Behavioral Advertising and How Can I Opt-out?

5. What About Information I Disclose Publicly?

- a. User Generated Content and Public Information
- b. Name and Likeness

6. Does Third Party Content And Links To Third Party Services Appear on Our Services

7. What about Social Media Features and Widgets?

8. How Do I Change My Information And What If I Cancel My Account?

9. What Should Parents Know About Children?

10. What About Security?

11. What About Changes To The Privacy Policy?

12. Your California Privacy Rights

13. What About Consent To Transfer Information To The United States?

1. What Information Do We Collect?

(a) Information You Provide To Us

Personal Information. We may ask you to provide us with certain categories of information such as personal information, which is information that could reasonably be used to identify you personally, such as your name, e-mail address, and mobile number ("Personal Information"). We may collect this information through various forms and in various places through

Complaint

Uber - Legal

<https://web.archive.org/web/20141018005925/https://www.uber.com/legal...>

the Services, including account registration forms, contact us forms, or when you otherwise interact with us. When you sign up to use the Services, you create a user profile. The current required data fields are:

- Email
- Password
- Name
- Mobile Phone Number
- Zip Code
- Credit Card Number, expiration date & security code and or information regarding your PayPal, Google Wallet or other digital payment accounts

If you choose to upload a photo when registering for our Services, the photo may be viewable by us and by the drivers who are picking you up so that they are able to verify your identity. You may remove or update the photo at any time by logging into your account.

(b) Information We Collect As You Access And Use Our Services

In addition to any Personal Information or other information that you choose to submit to us, we and our third-party service providers may use a variety of technologies that automatically (or passively) collect certain information whenever you visit or interact with the Services ("**Usage Information**"). This Usage Information may include the browser that you are using, the URL that referred you to our Services, all of the areas within our Services that you visit, and the time of day, among other information. We may use Usage Information for a variety of purpose , including to enhance or otherwise improve the Services. In addition, we collect your IP address or other unique identifier ("**Device Identifier**") for your computer, mobile or other device used to access the Services (any, a "**Device**"). A Device Identifier is a number that is automatically assigned to your Device used to access the Services, and our computers identify

Complaint

Uber - Legal

<https://web.archive.org/web/20141018005925/https://www.uber.com/legal...>

your Device by its Device Identifier. Usage Information may be non-identifying or may be associated with you. Whenever we associate Usage Information or a Device Identifier with your Personal Information, we will treat it as Personal Information.

In addition, tracking information is collected as you navigate through our Services, including, but not limited to geographic areas. If you are traveling in a vehicle requested via our Services, the driver's mobile phone will send your GPS coordinates, during the ride, to our servers. Most GPS enabled mobile devices can define one's location to within 50 feet. We collect this information for various purposes – including to determine the charge for the transportation you requested via our Services, to provide you with customer support, to send you promotions and offers, to enhance our Services, and for our internal business purposes. We may also have features that allow you to share this information with other people (such as your family, friends or colleagues) if you choose.

For example, when you choose to split the fare for a trip with other users, all users splitting the fare can see the GPS coordinates recorded by the driver's mobile phone for that particular trip, as well as certain information about the users (such as the User's name and photos) who have agreed to split the fare for that trip.

A few of the methods that may be used to collect Usage Information include, without limitation, the following (and subsequent technology and methods hereafter developed):

Cookies. A cookie is a data file placed on a Device when it is used to access the Services. A Flash cookie is a data file placed on a Device via the Adobe Flash plug-in that may be built-in to or downloaded by you to your Device. Cookies and Flash Cookies may be used for many purposes, including, without limitation, remembering you and your preferences and tracking your visits to our web pages. Cookies work by assigning a number to the

Complaint

Uber - Legal

<https://web.archive.org/web/20141018005925/https://www.uber.com/legal...>
user that has no meaning outside of the assigning website.

If you do not want information to be collected through the use of cookies, your browser allows you to deny or accept the use of cookies. Cookies can be disabled or controlled by setting a preference within your web browser or on your Device. If you choose to disable cookies or Flash cookies on your Device, some features of the Services may not function properly or may not be able to customize the delivery of information to you.

You should be aware that the Company cannot control the use of cookies (or the resulting information) by third-parties, and use of third party cookies is not covered by our Privacy Policy.

Web Beacons. Small graphic images or other web programming code called web beacons (also known as "1x1 GIFs" or "clear GIFs") may be included in our web and mobile pages and messages. The web beacons are tiny graphics with a unique identifier, similar in function to cookies, and are used to track the online movements of Web users. In contrast to cookies, which are stored in a user's computer hard drive, web beacons are embedded invisibly on Web pages and are about the size of the period at the end of this sentence. Web beacons or similar technologies help us better manage content on our Services by informing us what content is effective, count users of the Services, monitor how users navigate the Services, count how many e-mails that we send were actually opened or to count how many particular articles or links were actually viewed. We do not tie the information gathered by web beacons to our customers' personal information.

Embedded Scripts. An embedded script is programming code that is designed to collect information about your interactions with the Services, such as the links you click on. The code is temporarily downloaded onto your Device from our web server or a third party service provider, is active only while you are connected to the Services, and is deactivated or deleted

Complaint

Uber - Legal

<https://web.archive.org/web/20141018005925/https://www.uber.com/legal...>

thereafter.

(c) Information Third Parties Provide About You

We may, from time to time, supplement the information we collect about you through our web site or Mobile Application with outside records from third parties in order to enhance our ability to serve you, to tailor our content to you and to offer you opportunities to purchase products or services that we believe may be of interest to you. We may combine the information we receive from those sources with information we collect through the Services. In those cases, we will apply this Privacy Policy to any Personal Information received, unless we have disclosed otherwise.

(d) Information You Provide About A Third Party

If you choose to use our referral service to tell a friend about our Services or a job position, we will ask you for your friend's name and email address. We will automatically send your friend a one-time email inviting him or her to visit the Services. We store this information for the sole purpose of sending this one-time email and tracking the success of our referral program, and do not use this information for any other marketing purpose unless we obtain consent from that person or we explicitly say otherwise. Please be aware that when you use any send-to-a-friend functionality through our Services, your e-mail address may be included in the communication sent to your friend.

If you choose to split a trip fare, we will ask you for your friend's mobile number. We will send your friend a text message informing him or her that you have requested that he or she split the fare for a trip. Your friend may accept or decline your request to split your fare. We will not use this information for any marketing purpose unless we obtain consent from that person or we explicitly say otherwise.

Your friend may contact us through t.uber.com/support

Complaint

Uber - Legal

<https://web.archive.org/web/20141018005925/https://www.uber.com/legal...>
(/web/20141018005925/http://t.uber.com/support) to request that we remove this information from our database.

(e) Information Collected by Mobile Applications

Our Services are primarily provided through an application on your mobile, tablet computer or similar device ("**Mobile Application**"). You agree that we may collect and use technical data and related information, including but not limited to, technical information about your device, system and application software, and peripherals, that is gathered periodically to facilitate the provision of software updates, product support and other services to you (if any) related to such Mobile Applications.

When you use any of our Mobile Applications, the Mobile Application may automatically collect and store some or all of the following information from your mobile device ("**Mobile Device Information**"), including without limitation:

- Your preferred language and country site (if applicable)
- Your phone number or other unique device identifier assigned to your mobile device – such as the International Mobile Equipment Identity or the Mobile Equipment ID number
- The IP address of your mobile device
- The manufacturer and model of your mobile device
- Your mobile operating system
- The type of mobile Internet browsers you are using
- Your geolocation
- Information about how you interact with the Mobile Application and any of our web sites to which the Mobile Application links, such as how many times you use a specific part of the mobile application over a given time period, the amount of time you spend using the Mobile Application, how often you use the Mobile Application, actions you take in the Mobile Application and how you engage with the Mobile Application
- Information to allow us to personalize the services and content available through the Mobile Application

We may use information automatically collected by the Mobile

Complaint

Uber - Legal

<https://web.archive.org/web/20141018005925/https://www.uber.com/legal...>

Application (including the Mobile Device Information) in the following ways:

- To operate and improve our Mobile Applications, other Services, our company's services, and tools;
- To create aggregated and anonymized information to determine which Mobile Application features are most popular and useful to users, and for other statistical analyses;
- To prevent, discover and investigate violations of this Privacy Policy or any applicable terms of service or terms of use for the Mobile Application, and to investigate fraud, chargeback or other matters;
- To customize the content or services on the Mobile Application for you, or the communications sent to you through the Mobile Application.

With respect to geo-location data we track through your Mobile Device, we use that geo-location information for various purposes – including for you to be able to view the drivers in your area that are close to your location, for you to set your pick up location, so the drivers are able to find the location from which you wish to be picked up, to send you promotions and offers, and to allow you (if you choose through any features we may provide) to share this information with other people. Except as otherwise permitted in this Privacy Policy, we will not share this information with third parties for any purpose and will only use this information for the sole purpose of providing you with the ability to request transportation via Uber's Mobile Application. You may at any time no longer allow our Mobile Application to use your location by turning this feature off at the Mobile Device level.

We also provide some of your Personal Information (such as your first name and your photo, if you have chosen to upload your photo to your profile) to the driver/partner who accepts your request for transportation so that the driver may contact and find you, and to those users with whom you have agreed to split the fare for a particular trip. The companies for which drivers work (that are providing the transportation service) are also able to

Complaint

Uber - Legal

<https://web.archive.org/web/20141018005925/https://www.uber.com/legal...>

access your Personal Information, including your geo-location data.

We may associate your unique mobile Device Identifier or Mobile Application usage information with any Personal Information you provide, but we will treat the combined information as Personal Information.

Personal Information may also be collected and shared with third-parties if there is content from the Mobile Application that you specifically and knowingly upload to, share with or transmit to an email recipient, online community, website, or to the public, e.g. uploaded photos, posted reviews or comments, or information about you or your ride that you choose to share with others through features which may be provided on our Services. This uploaded, shared or transmitted content will also be subject to the privacy policy of the email, online community website, social media or other platform to which you upload, share or transmit the content.

(f) Information Collected from Job Applicants

If you wish to apply for a job on our web site(s), we will collect Personal Information such as your name, email address, phone number and may collect additional information such as resume, gender, and your ethnicity. We use the information collected within this area of the web site(s) to determine your qualifications for the position in which you have applied and to contact you to set up an interview.

2. How Do We Use The Information Collected?

Our primary goal in collecting your Personal information or Usage Information is to provide you with an enhanced experience when using the Services.

Based upon the Personal Information you provide us when

Complaint

Uber - Legal

<https://web.archive.org/web/20141018005925/https://www.uber.com/legal...>

registering for an account, we will send you a welcoming email to verify your username and password. We will also communicate with you in response to your inquiries, to provide the services you request, and to manage your account. We will communicate with you by email, telephone, or SMS or text message, in accordance with your wishes.

We use your information to closely monitor which features of the Services are used most, to allow you to view your trip history, store your credit card information on a secure page, view any promotions we may currently be running, rate trips, and to determine which features we need to focus on improving, including usage patterns and geographic locations to determine where we should offer or focus services, features and/or resources.

We use the information collected from our Mobile Application so that we are able to serve you the correct app version depending on your device type, for troubleshooting and in some cases, marketing purposes. The credit card information you provide in your personal profile at sign-up is not stored by us, but is stored and used by our third party credit card processors in order for them to process payment that you owe third parties for transportation services received by you.

We use your Internet Protocol (IP) address to help diagnose problems with our computer server, and to administer our web site(s). Your IP address is used to help identify you, but contains no personal information about you.

We will send you strictly service-related announcements on rare occasions when it is necessary to do so. For instance, if our Services are temporarily suspended for maintenance, we might send you an email. Generally, you may not opt-out of these communications, which are not promotional in nature. If you do not wish to receive them, you have the option to deactivate your account.

Complaint

Uber - Legal

<https://web.archive.org/web/20141018005925/https://www.uber.com/legal...>

In addition, we may use your Personal Information or Usage Information that we collect about you: (1) to provide you with information or services or process transactions that you have requested or agreed to receive including to send you electronic newsletters, or to provide you with special offers or promotional materials on behalf of us or third parties; (2) to process your registration with the Services, including verifying your information is active and valid; (3) to improve the Services or our services, to customize your experience with the Services, or to serve you specific content that is most relevant to you; (4) to enable you to participate in a variety of the Services' features such as online or mobile entry sweepstakes, contests or other promotions; (5) to contact you with regard to your use of the Services and, in our discretion, changes to the Services and/or the Services' policies; (6) for internal business purposes; (7) for inclusion in our data analytics; and (8) for purposes disclosed at the time you provide your information or as otherwise set forth in this Privacy Policy.

Please note that information submitted to the Services via a "contact us" or other similar function may not receive a response.

3. How and When Do We Disclose Information to Third Parties?

We may share non-personally identifiable information, such as aggregated user statistics and log data, with third parties for industry analysis, demographic profiling, to deliver targeted advertising about other products or services, or for other business purposes. We do not sell, share, rent or trade the information we have collected about you, including Personal Information, other than as disclosed within this Privacy Policy or at the time you provide your information. We do not share your Personal Information with third parties for those third parties' direct marketing purposes unless you consent to such sharing at the time you provide your Personal Information.

(a) When You Agree To Receive Information From Third Parties.

Complaint

Uber - Legal

<https://web.archive.org/web/20141018005925/https://www.uber.com/legal...>

You may be presented with an opportunity to receive information and/or marketing offers directly from third parties. If you do agree to have your Personal Information shared, your Personal Information will be disclosed to such third parties and all information you disclose will be subject to the privacy policy and practices of such third parties. We are not responsible for the privacy policies and practices of such third parties and, therefore, you should review the privacy policies and practices of such third parties prior to agreeing to receive such information from them. If you later decide that you no longer want to receive communication from a third party, you will need to contact that third party directly.

(b) Third Parties Providing Services on Our Behalf.

We use third party companies and individuals to facilitate our Services, provide or perform certain aspects of the Services on our behalf – such as drivers and companies they work for to provide the Services, and other third-parties to host the Services, design and/or operate the Services' features, track the Services' analytics, process payments, engage in anti-fraud and security measures, provide customer support, provide geo-location information to our drivers, enable us to send you special offers, host our job application form, perform technical services (e.g., without limitation, maintenance services, database management, web analytics and improvement of the Services' features), or perform other administrative services. We may provide these vendors with access to user information, including Personal Information, this information sharing is limited to only the information needed by the vendor to carry out the services they are performing for you or for us. Each of these vendors are obligated not to disclose or use Personal Information for any other purpose.

While we may use third party analytics service providers to evaluate and provide us with information about the use of the Services and viewing of our content, we do not share Personal Information with these analytics service providers, but they may

Complaint

Uber - Legal

<https://web.archive.org/web/20141018005925/https://www.uber.com/lega...>

set and access their own cookies, web beacons and embedded scripts on your Device and they may otherwise collect or have access to information about you, including non-personally identifiable information.

We use a third party hosting provider who hosts our support section of our website. Information collected within this section of our web site is governed by our Privacy Policy.

(c) Co-branded Services.

Certain aspects of the Services may be provided to you in association with third parties ("**Co-Branded Services**") such as sponsors and charities, and may require you to disclose Personal Information to them. Such Co-Branded Services will identify the third party. If you elect to register for products and/or services through the Co-Branded Services, you may be providing your information to both us and the third party. Further, if you sign-in to a Co-Branded Service with a username and password obtained through our Services, your Personal Information may be disclosed to the identified third parties for that Co-Branded Service and will be subject to their posted privacy policies.

(d) Sweepstakes, Contests and Promotions.

We may offer sweepstakes, contests, and other promotions (any, a "**Promotion**") through the Services that may require registration. By participating in a Promotion, you are agreeing to official rules that govern that Promotion, which may contain specific requirements of you, including, allowing the sponsor of the Promotion to use your name, voice and/or likeness in advertising or marketing associated with the Promotion. If you choose to enter a Promotion, Personal Information may be disclosed to third parties or the public in connection with the administration of such Promotion, including, in connection with winner selection, prize fulfillment, and as required by law or permitted by the Promotion's official rules, such as on a winners list.

Complaint

Uber - Legal

<https://web.archive.org/web/20141018005925/https://www.uber.com/legal...>

(e) Administrative and Legal Reasons.

We cooperate with government and law enforcement officials and private parties to enforce and comply with the law. Thus, we may access, use, preserve, transfer and disclose your information (including Personal Information), including disclosure to third parties such as government or law enforcement officials or private parties as we reasonably determine is necessary and appropriate: (i) to satisfy any applicable law, regulation, subpoenas, governmental requests or legal process; (ii) to protect and/or defend the Terms and Conditions ([/web/20141018005925/https://www.uber.com/legal/terms](https://web/20141018005925/https://www.uber.com/legal/terms)) for online and mobile Services or other policies applicable to any online and mobile Services, including investigation of potential violations thereof; (iii) to protect the safety, rights, property or security of the Company, our Services or any third party; (iv) to protect the safety of the public for any reason; (v) to detect, prevent or otherwise address fraud, security or technical issues; and/or (vi) to prevent or stop activity we may consider to be, or to pose a risk of being, an illegal, unethical, or legally actionable activity. Further, we may use IP address or other Device Identifiers, to identify users, and may do so in cooperation with third parties such as copyright owners, internet service providers, wireless service providers and/or law enforcement agencies, including disclosing such information to third parties, all in our discretion. Such disclosures may be carried out without notice to you.

(f) Business Transfer.

We may share your information, including your Personal Information and Usage Information with our parent, subsidiaries and affiliates for internal reasons. We also reserve the right to disclose and transfer all such information: (i) to a subsequent owner, co-owner or operator of the Services or applicable database; or (ii) in connection with a corporate merger, consolidation, restructuring, the sale of substantially all of our membership interests and/or assets or other corporate change,

Complaint

Uber - Legal

<https://web.archive.org/web/20141018005925/https://www.uber.com/legal...>

including, during the course of any due diligence process.

4. What is Online Behavioral Advertising and How Can I Opt-Out?

Targeted advertising (also known as Behavioral Advertising) uses information collected on an individual's web or mobile browsing behavior such as the pages they have visited or the searches they have made. This information is then used to select which advertisements should be displayed to a particular individual on websites other than our web site(s). For example, if you have shown a preference for nursing while visiting our web site(s), you may be served an advertisement for nursing-related programs when you visit a site other than our web site(s). The information collected is only linked to an anonymous cookie ID (alphanumeric number); it does not include any information that could be linked back to a particular person, such as their name, address or credit card number. The information used for targeted advertising either comes from us or through third party website publishers.

If you would like to opt out of targeted advertising from us that occurs when visiting our third party advertising publishers, please click here ([/web/20141018005925/http://www.networkadvertising.org/managing/opt_out.asp](https://web.archive.org/web/20141018005925/http://www.networkadvertising.org/managing/opt_out.asp)) to access the NAI Opt-Out Page. Please note that this will opt you out of targeted ads from our Company and any other participating advertisers. If you opt out, you may continue to receive online advertising from us; however, these ads may not be as relevant to you.

In order for behavioral advertising opt-outs to work on your Device, your browser must be set to accept cookies. If you delete cookies, buy a new Device, access our Services from a different device, login under a different screen name, or change web browsers, you will need to opt-out again. If your browser has

Complaint

Uber - Legal

<https://web.archive.org/web/20141018005925/https://www.uber.com/legal...>

scripting disabled, you do not need to opt out, as online behavioral advertising technology does not work when scripting is disabled. Please check your browser's security settings to validate whether scripting is active or disabled.

Additionally, many network advertising programs allow you to view and manage the interest categories they have compiled from your online browsing activities. These interest categories help determine the types of targeted advertisements you may receive. The NAI Opt-Out Page provides a tool that identifies its member companies that have cookies on your browser and provides links to those companies.

5. What About Information I Disclose Publicly?

(a) User Generated Content and Public Information.

The Services may offer publicly accessible blogs or community forums or other ways to permit you to submit ideas, photographs, user profiles, writings, music, video, audio recordings, computer graphics, pictures, data, questions, comments, suggestions or other content, including Personal Information (collectively, "User Content"). We or others may reproduce, publish, distribute or otherwise use User Content online or offline in any media or format (currently existing or hereafter developed). Others may have access to this User Content and may have the ability to share it with third parties across the Internet. You should be aware that any User Content you provide in these areas may be read, collected, and use by others who access them. Thus, please think carefully before deciding what information you share, including Personal Information, in connection with your User Content. Please note that Company does not control who will have access to the information that you choose to make public, and cannot ensure that parties who have access to such publicly available information will respect your privacy or keep it secure. This Privacy Policy does not apply to any information that you disclose publicly, share with others or otherwise upload,

Complaint

Uber - Legal

<https://web.archive.org/web/20141018005925/https://www.uber.com/legal...>

whether through the Services or otherwise. We are not responsible for the accuracy, use or misuse of any content or information that you disclose or receive through the Services.

To request removal of your User Content from our blog or community forum or similar features, contact us through t.uber.com/support ([/web/20141018005925/http://t.uber.com/support](https://web/20141018005925/http://t.uber.com/support)). In some cases, we may not be able to remove your User content, in which case we will let you know if we are unable to do so and why.

(b) Name and Likeness.

We may also publish your name, voice, likeness and other Personal Information that is part of your User Content, and we may use the content, or any portion of the content, for advertising, marketing, publicity and promotional activities. For full terms and conditions regarding User Content you submit to the Services, please review our Terms and Conditions ([/web/20141018005925/https://www.uber.com/legal/terms](https://web/20141018005925/https://www.uber.com/legal/terms)).

6. Does Third Party Content And Links To Third Party Services Appear on the Services?

The Services may contain content that is supplied by a third party, and those third parties may collect web site usage information and your Device Identifier when web pages from any online or mobile Services are served to your browser. In addition, when you are using the Services, you may be directed to other sites or applications that are operated and controlled by third parties that we do not control. We are not responsible for the privacy practices employed by any of these third parties. For example, if you click on a banner advertisement, the click may take you away from one of our websites onto a different web site. These other web sites may send their own cookies to you, independently collect data or solicit Personal Information and may or may not have their own published privacy policies. We

Complaint

Uber - Legal

<https://web.archive.org/web/20141018005925/https://www.uber.com/legal...>

encourage you to note when you leave our Services and to read the privacy statements of all third party web sites or applications before submitting any Personal Information to third parties.

7. What About Social Media Features and Widgets?

Our online and mobile Services may include social media features, such as the Facebook Like button, and widgets such as a "Share This" button, or interactive mini-programs that run on our online and mobile Services. These features may collect your IP address, which page you are visiting on our online or mobile Services, and may set a cookie to enable the feature to function properly. Social media features and widgets are either hosted by a third party or hosted directly on our online Services. Your interactions with these features and widgets are governed by the privacy policy of the company providing them.

8. How Do I Change My Information and What If I Cancel My Account?

You are responsible for maintaining the accuracy of the information you submit to us, such as your contact information provided as part of account registration. If your Personal Information changes, or if you no longer desire our Services, you may correct, delete inaccuracies, or amend information by making the change on our member information page or by contacting us through t.uber.com/support ([/web/20141018005925/http://t.uber.com/support](https://web/20141018005925/http://t.uber.com/support)). We will make good faith efforts to make requested changes in our then active databases as soon as reasonably practicable.

You may also cancel or modify your communications that you have elected to receive from the Services by following the instructions contained within an e-mail or by logging into your user account and changing your communication preferences.

Complaint

Uber - Legal

<https://web.archive.org/web/20141018005925/https://www.uber.com/legal...>

If you wish to cancel your account or request that we no longer use your information to provide you services, contact us through t.uber.com/support ([/support](https://web/20141018005925/http://t.uber.com/support)).

We will retain your Personal Information and Usage Information (including geo-location) for as long as your account with the Services is active and as needed to provide you services. Even after your account is terminated, we will retain your Personal Information and Usage Information (including geo-location, trip history, credit card information and transaction history) as needed to comply with our legal and regulatory obligations, resolve disputes, conclude any activities related to cancellation of an account (such as addressing chargebacks from your credit card companies), investigate or prevent fraud and other inappropriate activity, to enforce our agreements, and for other business reason. After a period of time, your data may be anonymized and aggregated, and then may be held by us as long as necessary for us to provide our Services effectively, but our use of the anonymized data will be solely for analytic purposes.

9. What Should Parents Know About Children?

The Company cares about the safety of children. Because our Services are not directed toward minors, no one under 18 (and certainly no children under 13) are allowed to register with or use the Services. We do not knowingly collect personal information from anyone under the age of 18. If we discover that we have collected personal information from a person under 18, we will delete that information immediately. If you are a parent or guardian of a minor under the age of eighteen (18) and believe he or she has disclosed Personal Information to us, please contact us at privacy@uber.com. (<mailto:privacy@uber.com>).

10. What About Security?

The Personal Information and Usage Information we collect is

Complaint

Uber - Legal

<https://web.archive.org/web/20141018005925/https://www.uber.com/legal...>

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 (we do not ourselves retain your entire credit card information) and geo-location information. However, as effective as encryption technology is, no security system is impenetrable. We cannot guarantee the security of our databases, nor can we guarantee that information you supply won't be intercepted while being transmitted to us over the Internet or wireless communication, and any information you transmit to the Company you do at your own risk. We recommend that you not disclose your password to anyone.

11. What About Changes To The Privacy Policy?

From time to time, we may update this Privacy Policy to reflect changes to our information practices. Any changes will be effective immediately upon the posting of the revised Privacy Policy. If we make any material changes, we will notify you by email (sent to the e-mail address specified in your account) or by means of a notice on the Services prior to the change becoming effective. We encourage you to periodically review this page for the latest information on our privacy practices.

12. Your California Privacy Rights

California's "Shine the Light" law, California Civil Code § 1798.83, requires certain businesses to respond to requests from California customers (those who have an established business relationship with us) asking about the business' practices related to disclosing personal information to third parties for the third parties' direct marketing purposes. Alternately, such businesses may have in place a policy not to disclose personal information of customers to third parties for the third parties' direct marketing purposes unless the customer first affirmatively agrees to the disclosure (opt-in) or if the customer has exercised an option to

Complaint

Uber - Legal

<https://web.archive.org/web/20141018005925/https://www.uber.com/legal...>

opt-out of such information-sharing (opt-out).

We have opted for this alternative approach, and we do not share personal information of customers information to third parties for the third parties' direct marketing purposes unless you provide us with permission at the time you provide such customer information.

13. What About Consent To Transfer Information To The United States?

If you are located anywhere outside of the United States, please be aware that information we collect, including, Personal Information, will be transferred to, processed and stored in the United States. The data protection laws in the United States may differ from those of the country in which you are located, and your Personal Information may be subject to access requests from governments, courts, or law enforcement in the United States according to laws of the United States. By using the Services or providing us with any information, you consent to this transfer, processing and storage of your information in the United States.

DOWNLOAD UBER (WEB/20141018005925/HTTPS://WWW.UBER.COM/APP)

Complaint

Uber - Legal

<https://web.archive.org/web/20141018005925/https://www.uber.com/legal...>

(/WEB/20141018005925/HTTPS://WWW.UBER.COM/SIGN-UP)

f ↓ (/web/20141018005925/https://www.facebook.com/uber)
t ↓ (/web/20141018005925/https://twitter.com/uber)
in ↓ (/web/20141018005925/https://www.linkedin.com/company/1815218)
g+ ↓ (/web/20141018005925/https://plus.google.com/112684473482252498171)

HOME (/WEB/20141018005925/HTTPS://WWW.UBER.COM/) • CITIES (/WEB/20141018005925/HTTPS://WWW.UBER.COM/CITIES) • DRIVE (/WEB/20141018005925/HTTPS://PARTNERS.UBER.COM/DRIVE)

HELP CENTER (/WEB/20141018005925/HTTPS://SUPPORT.UBER.COM) CAREERS (/WEB/20141018005925/HTTPS://WWW.UBER.COM/JOBS) DEVELOPERS (/WEB/20141018005925/HTTPS://DEVELOPER.UBER.COM) BLOG (/WEB/20141018005925/HTTPS://BLOG.UBER.COM) ABOUT US (/WEB/20141018005925/HTTPS://WWW.UBER.COM/ABOUT)

ENGLISH

Decision and Order

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.

Decision and Order

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

Decision and Order

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

Decision and Order

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:

Decision and Order

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.

Decision and Order

- 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.

Decision and Order

- 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;

Decision and Order

- 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.

Concurring Statement

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.

**STATEMENT OF
COMMISSIONER ROHIT CHOPRA**

Uber’s business model relies on users and drivers trusting that the company will take care to protect their most sensitive information, including Social Security numbers, geolocation information, driver’s license information, and proof of insurance. This case calls into question whether the company deserves that trust.

As recounted in the Commission’s Complaint, Uber misled law enforcement even as it was under investigation for misleading the public about its security practices. Specifically, in the midst of the Commission’s investigation, Uber experienced a *second* serious breach – a breach rooted in the very slipshod security practices already being investigated. Rather than informing the Commission or the public of this second attack on its systems, Uber apparently paid the attackers to sweep it under the rug, waiting more than a year after learning of the breach before informing the public or the Commission.¹

Given the serious misconduct uncovered in this investigation, I support this action. But, I believe the Commission should have given greater weight to several of the suggestions made in the comments.²

In particular, I agree with World Privacy Forum and EPIC that the Commission should make required audits and assessments public, subject to appropriate redactions. The FTC has responded to this comment by stating that these documents are available by filing a Freedom of

1 This and other events of the last several years raise serious questions about the company’s culture, corporate governance, and commitment to following the law. As recently as 2017, the company agreed to pay \$20 million to settle FTC charges that it misled prospective drivers with exaggerated earning claims. And according to our Complaint in this matter, Uber reportedly created a tracking tool – “God view” – to surveil the whereabouts of its riders. Another report detailed a company executive’s desire to target critical journalists with opposition research.

2 The comments also suggested that we further define privacy assessments/audits and that we seek deletion or “disgorgement” of ill-gotten data. The comments are available at <https://www.ftc.gov/policy/public-comments/2018/05/initiative-754>.

Concurring Statement

Information Act request, but proactive disclosure would be superior, given the public interest in keeping this company in compliance.

Statement of Commissioner Rebecca Kelly Slaughter

I support the action announced today to give final approval to an administrative consent order with Uber Technologies, Inc., resolving charges that the company deceived consumers regarding its privacy and data security practices. Notably, the consent order imposes additional obligations on Uber in light of the fact that the company failed to inform the FTC that it had suffered a significant data breach during the course of the agency's investigation of a similar prior breach.

While I believe that the injunctive provisions in the order will provide strong protections for consumers and their personal information, I also believe that the FTC should have additional authority and remedies to address deceptive or unfair conduct relating to privacy and data security. Namely, we do not have the ability to issue rules under the Administrative Procedures Act that would provide additional guidance for how companies must treat data, nor do we have the ability to assess civil penalties against companies that violate the FTC Act in connection with their data practices. The threat of civil penalties would provide a greater incentive to firms to follow through on the promises they make to consumers and to make appropriate investments to implement reasonable data security safeguards.

In a high-profile case such as this, which has been the subject of significant public attention and press reports, many stakeholders understandably are interested in Uber's future conduct and its compliance with this order. The FTC's Division of Enforcement is responsible for monitoring compliance under all federal and administrative court orders that are still in effect pertaining to consumer protection matters. The agency's compliance monitoring efforts include not just the review of formal reports and assessments that are required under orders, but in many instances also include a continuous open channel of communication between attorneys in the Division of Enforcement and representatives of the companies under order regarding both past and future business practices. These ongoing compliance efforts are non-public.

Two public comments submitted on the proposed consent order requested that the Commission proactively release copies of the third-party privacy assessments Uber is required to provide to the Commission under the order. While these assessments are available to any requester in response to a FOIA request, I would have preferred to see the proactive release of the assessments in this specific case due to the objectively high level of public interest in this matter, including in the assessments in particular. However, I want to emphasize that any privacy or data security assessment that is released to the public – through FOIA or any other means – will not provide a complete picture of a company's compliance under an FTC order, or the

Analysis to Aid Public Comment

FTC's efforts in monitoring that company's compliance. This is not simply because such reports must be redacted to protect proprietary information, but because the FTC's compliance monitoring efforts in many cases extend far beyond what can be gleaned from an isolated assessment.

ANALYSIS OF CONSENT ORDER TO AID PUBLIC COMMENT

The Federal Trade Commission has withdrawn its acceptance of the agreement containing consent order from Uber Technologies, Inc. ("Uber") that the Commission released for public comment in this proceeding on August 15, 2017 ("August 2017 proposed consent agreement"), and has accepted, subject to final approval, a new agreement containing consent order from Uber ("April 2018 proposed consent agreement").

The April 2018 proposed consent agreement has been placed on the public record for thirty (30) days for receipt of comments by interested persons. All comments received during this period will become part of the public record. Interested persons who submitted comments during the public comment period for the August 2017 proposed consent agreement should resubmit their original comments, or submit new comments, during the new comment period if they would like the Commission to consider their comments when the Commission decides whether to make final the April 2018 proposed consent agreement. After thirty (30) days, the Commission again will review the April 2018 proposed consent 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 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

Analysis to Aid Public Comment

“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. 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. Count one of 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 2016.¹

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 in the Amazon S3 Datastore a variety of files 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.

¹ Count one of the proposed complaint and the underlying factual allegations are unchanged from the proposed complaint against Uber that the Commission issued previously as part of the August 2017 proposed consent agreement.

Analysis to Aid Public Comment

As described below, count two of 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.² Specifically, Uber allegedly:

- Failed to implement reasonable access controls to safeguard data stored in the Amazon S3 Datastore. For example, Uber (1) until approximately September 2014, 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) until approximately September 2014, failed to restrict access to systems based on employees' job functions; and (3) until approximately September 2015, failed to require multi-factor authentication for individual account access, and until at least November 2016, failed to require multi-factor authentication for programmatic service account access, to the Amazon S3 Datastore;
- Until at least September 2014, failed to implement reasonable security training and guidance;
- Until approximately September 2014, failed to have a written information security program; and
- Until at least November 2016, stored sensitive personal information in the Amazon S3 Datastore in clear, readable text, rather than encrypting the information.

As a result of these failures, intruders accessed Uber's Amazon S3 Datastore multiple times using access keys that Uber engineers had posted to GitHub, a code-sharing site used by software developers.

First, on or about May 12, 2014, an intruder accessed Uber's Amazon S3 Datastore using an access key that was publicly posted and granted full administrative privileges to all data and documents stored within Uber's Amazon S3 Datastore (the "2014 data breach"). 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. Uber sent breach notification letters to affected Uber Drivers in February 2015. Uber later learned of more

² Count two of the proposed complaint addresses the same allegedly false or misleading statements as did count two of the proposed complaint against Uber that the Commission issued as part of the August 2017 proposed consent agreement. The proposed complaint includes allegations that the now withdrawn complaint included to support count two and also includes additional allegations to support count two based on new information the Commission obtained after August 2017.

Analysis to Aid Public Comment

affected Uber Drivers in May and July 2016 and sent breach notification letters to those Drivers in June and August 2016.

Second, between October 13, 2016 and November 15, 2016, intruders accessed Uber's Amazon S3 Datastore using an AWS access key that was posted to a private GitHub repository ("the 2016 data breach"). Uber granted its engineers access to Uber's GitHub repositories through engineers' individual GitHub accounts, which engineers generally accessed through personal email addresses. Uber did not have a policy prohibiting engineers from reusing credentials, and did not require engineers to enable multi-factor authentication when accessing Uber's GitHub repositories. The intruders who committed the 2016 breach said that they accessed Uber's GitHub page using passwords that were previously exposed in other large data breaches, whereupon they discovered the AWS access key they used to access and download files from Uber's Amazon S3 Datastore. The intruders downloaded sixteen files that contained unencrypted consumer personal information relating to U.S. Riders and Drivers, including approximately 25.6 million names and email addresses, 22.1 million names and mobile phone numbers, and 607,000 names and driver's license numbers. Nearly all of the exposed personal information was collected before July 2015 and stored in unencrypted database backup files.

Uber discovered the 2016 data breach on or about November 14, 2016, when one of the attackers contacted Uber claiming to have compromised Uber's "databases" and demanding a six-figure payout. Uber paid the attackers \$100,000 through the third party that administers Uber's "bug bounty" program. Respondent created the bug bounty program to pay financial rewards in exchange for the responsible disclosure of serious security vulnerabilities. However, the attackers who committed the 2016 data breach were fundamentally different from legitimate bug bounty recipients. Instead of responsibly disclosing a vulnerability, the attackers maliciously exploited the vulnerability and acquired millions of consumers' personal information.

Uber failed to disclose the 2016 data breach to affected consumers until November 21, 2017, more than a year after discovering it. Uber also failed to disclose the 2016 data breach to the Commission until November 2017 despite the fact that the breach occurred in the midst of a nonpublic Commission investigation relating to Uber's data security practices, including, specifically, the security of Uber's Amazon S3 Datastore.

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

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. This Part is identical to Part I of the August 2017 proposed consent agreement.

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)

Analysis to Aid Public Comment

protect the privacy and confidentiality of consumers' personal information. Part II.B includes new language that requires Uber's mandated privacy risk assessments to include consideration of risks and safeguards related to (a) secure software design, development, and testing, including access key and secret key management and secure cloud storage; (b) review, assessment, and response to third-party security vulnerability reports, including through a "bug bounty" or similar program; and (c) prevention, detection, and response to attacks, intrusions, or systems failures.

Part III of the proposed order requires Uber to undergo biennial assessments of its mandated privacy program by a third party. Part III has been revised from the August 2017 proposed consent agreement to require Uber to submit to the Commission each of its assessments rather than only its initial assessment.

Part IV of the proposed order requires Uber to submit a report to the Commission if Uber discovers any "covered incident" involving unauthorized access or acquisition of consumer information. This Part is new.

Parts V through IX of the proposed order are reporting and compliance provisions. 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 who participate in conduct related to the subject matter of the order, including all employees, agents, and representatives who regularly access personal information. Part VI mandates that Uber submit a compliance report to the FTC one year after issuance of the order and submit additional notices as specified. Parts VII and VIII require Uber to retain documents relating to its compliance with the order, and to provide such additional information or documents as are necessary for the Commission to monitor compliance. Part IX states that the order will remain in effect for 20 years.

These provisions include modifications from the August 2017 proposed consent agreement. Part V expands the acknowledgement of order provision to require Uber to obtain signed acknowledgements from all employees, agents, and representatives who regularly access personal information that Uber collects or receives from or about consumers, rather than limiting the requirement to employees with managerial responsibility related to the order. And Part VII contains modified recordkeeping provisions and new recordkeeping provisions relating to Uber's bug bounty program and its subpoenas and communications with law enforcement.

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.

Opinion of the Commission

IN THE MATTER OF

1-800 CONTACTS, INC.

OPINION OF THE COMMISSION AND FINAL ORDER IN REGARD TO ALLEGED VIOLATIONS OF
SECTION 5 OF THE FEDERAL TRADE COMMISSION ACT

Docket No. 9372; File No. 141 0200
Complaint, August 8, 2016 – Decision, November 7, 2018

This case addresses 1-800 Contacts, Inc.’s settlement agreements with over a dozen rivals prohibiting both 1-800 and the other parties from bidding on keywords containing the other’s trademarks, and requiring each party to implement negative keywords to ensure that their ads do not appear in search engine results pages for searches that contain each other’s trademarks. The complaint, 164 F.T.C. 360, alleges that these agreements are in restraint of trade in violation of Section 5 of the Federal Trade Commission Act. In his Initial Decision, 164 F.T.C. 373, the Administrative Law Judge found that the challenged agreements pose significant, unjustified anticompetitive consequences in the relevant market for the sale of contact lenses online. The Administrative Law Judge ordered 1-800 Contacts to cease and desist from enforcing or attempting to enforce any and all provisions, terms, or requirements in an existing agreement or court order that impose a condition on a Seller, which prohibits, restricts, regulates, or otherwise places any limitation on truthful, non-deceptive, and non-infringing advertising or promotion. *Id.* at 637. The Respondent appealed the Initial Decision. The Commission scheduled oral argument, 165 F.T.C. 1415, and subsequently rescheduled the arguments, 165 F.T.C. 1471. The Commission heard oral arguments on June 26, 2018.

Participants

For the *Commission*: Gustav Chiarello, Kathleen Clair, Joshua Barton Gray, Stuart Hirschfeld, Nathaniel Hopkin and Charlotte Slaiman.

For the *Respondent*: Garth Vincent, Munger Tolles & Olson; Darryl Nirenberg, Steptoe & Johnson.

OPINION OF THE COMMISSION

By Chairman Joseph J. Simons, for the Commission:

This proceeding considers Complaint Counsel’s challenge to a number of agreements among horizontal competitors—in most instances, trademark litigation settlements—that, allegedly, anticompetitively limit internet search advertising and restrict bidding in internet search auctions to the detriment of consumers. Respondent 1-800 Contacts sued rival contact-lens sellers for trademark infringement when sellers’ online advertising appeared in response to consumers’ internet searches for “1-800 Contacts.” In nearly all cases, the litigation settled before trial. The resulting settlement agreements require the parties, when bidding at search engine advertising auctions, to take steps to ensure their ads do not appear in response to searches for the other party’s trademark terms.

At first glance, this proceeding may appear to contemplate little more than a few terms embedded in a document that purports to resolve a trademark dispute among internet sellers of