epic.org

Electronic Privacy Information Center
1718 Connecticut Avenue NW, Suite 200
Washington, DC 20009, USA

+1 202 483 1140
+1 202 483 1248
@EPICPrivacy
https://epic.org

COMMENTS OF THE ELECTRONIC PRIVACY INFORMATION CENTER

to the

FEDERAL TRADE COMMISSION

In the Matter of Uber Technologies, Inc.

FTC File No. 152-3054

May 14, 2018

By notice published on April 25, 2018, the Federal Trade Commission has proposed a modified Consent Order with Uber Technologies, Inc. to settle charges that Uber misrepresented its privacy and data security practices.[1] Pursuant to this notice, the Electronic Privacy Information Center ("EPIC") submits these comments and recommendations to ensure that the final order adequately protects consumers and addresses the issues raised in the FTC's Complaints.

EPIC is a public interest research center in Washington, D.C. established in 1994 to focus public attention on emerging civil liberties issues and to protect privacy, the First Amendment, and constitutional values. EPIC has played a leading role in developing the authority of the FTC to address emerging privacy issues and to safeguard the privacy rights of consumers.[2] EPIC

[1] Uber Technologies, Inc.; Analysis to Aid Public Comment, 83 Fed. Reg. 18,061 (Apr. 25 2018), https://www.federalregister.gov/documents/2018/04/25/2018-08600/uber-technologies-inc-analysis-to-aid-public-comment [hereinafter "Analysis To Aid Public Comment"].

[2] See, e.g., Letter from EPIC Executive Director Marc Rotenberg to FTC Commissioner Christine Varney, EPIC (Dec. 14, 1995) (urging the FTC to investigate the misuse of personal information by the direct marketing industry) available at http://epic.org/privacy/internet/ftc/ftc_letter.html; EPIC, In the Matter of DoubleClick, Complaint and Request for Injunction, Request for Investigation and for Other Relief, before the Federal Trade Commission (Feb. 10, 2000), available at

routinely files complaints with the FTC regarding practices that threaten consumer privacy.[3] EPIC's 2009 and 2010 Complaints against Facebook led to the FTC's 2011 Consent Order with Facebook,[4] and EPIC's 2010 Complaint concerning Google Buzz was the basis for the FTC's 2011 Consent Order with Google.[5]

In 2015, EPIC filed a detailed complaint with the FTC against Uber, alleging many of the same privacy violations that the FTC found in its Complaint against Uber.[6] In response to the FTC's August 2017 proposed settlement with Uber, EPIC submitted detailed comments on how the FTC should strengthen the settlement.[7]

EPIC supports the FTC's decision to modify the August 2017 proposed Consent Order. To EPIC's knowledge, this marks the first time that the FTC has actually modified a proposed settlement following solicitation of public comments. However, the modified Order still falls

---

http://epic.org/privacy/internet/ftc/DCLK_complaint.pdf; EPIC, In the Matter of Microsoft Corporation, Complaint and Request for Injunction, Request for Investigation and for Other Relief, before the Federal Trade Commission (July 26, 2001), available at http://epic.org/privacy/consumer/MS_complaint.pdf; EPIC, In the Matter of Choicepoint, (Complaint, Request for Investigation and for Other Relief), Dec. 16, 2004, available at http://epic.org/privacy/choicepoint/fcraltr12.16.04.html.

[3] *See*, *e.g.* In the Matter of Google Inc. (Complaint, Request for Investigation, Injunction, and Other Relief), Jul 31, 2017, https://www.epic.org/privacy/ftc/google/EPIC-FTC-Google-Purchase-Tracking-Complaint.pdf; In the Matter of Genesis Toys and Nuance Communications (Complaint and Request for Investigation, Injunction, and Other Relief), Dec. 6, 2016, https://epic.org/privacy/kids/EPIC-IPR-FTC-Genesis-Complaint.pdf; In the Matter of Snapchat (Complaint, Request for Investigation, Injunction and Other Relief) May, 16, 2013, https://epic.org/privacy/ftc/EPIC-Snapchat-Complaint.pdf; In the Matter of Google, Inc. (Complaint, Request for Investigation, Injunction, and Other Relief), Feb. 16, 2010, https://epic.org/privacy/ftc/googlebuzz/GoogleBuzz_Complaint.pdf; In the Matter of Facebook (Complaint, Request for Investigation, Injunction, and Other Relief), Dec. 17, 2009, https://epic.org/privacy/inrefacebook/EPIC-FacebookComplaint.pdf.

[4] *See*, Fed. Trade Comm'n., *Facebook Settles FTC Charges That It Deceived Consumers By Failing To Keep Privacy Promises*, Press Release, (Nov. 9, 2011), https://www.ftc.gov/news-events/press-releases/2011/11/facebook-settles-ftc-charges-it-deceived-consumers-failing-keep ("Facebook's privacy practices were the subject of complaints filed with the FTC by the Electronic Privacy Information Center and a coalition of consumer groups.")

[5] *See*, EPIC, *In re Google Buzz*, http://epic.org/privacy/ftc/googlebuzz/.

[6] In the Matter of Uber Technologies, Inc. (2015) (Complaint, Request for Investigation, Injunction, and Other Relief), Jun. 22, 2015, https://epic.org/privacy/internet/ftc/uber/Complaint.pdf [hereinafter "EPIC Uber Complaint"].

[7] Comments of EPIC, *In the Matter of Uber Technologies, Inc.*, FTC File No. 152-3054, (Sep. 15, 2017), https://epic.org/apa/comments/EPIC-FTC-Uber-Settlement.pdf.

short in significant ways. According to the FTC's revised Complaint, Uber hid a massive data breach while the FTC was conducting its investigation into the company's data security practices.[8] Uber continued to hide this breach from the FTC and the public even after the FTC had charged the company with deceiving consumers about its data security practices. Given Uber's repeated misrepresentations about its data security practices, the FTC should make Uber's privacy assessments public so that consumers can evaluate whether the company is meeting its obligations under the Consent Order.

In addition, EPIC renews the recommendations we made in our September 2017 comments, which would ensure that Uber does not continue to violate the privacy and data security of its millions of consumers. The modified settlement should:

- Require Uber to provide consumers with access to the personal data maintained by Uber;
- Prohibit Uber from tracking consumers and accessing contact lists when they are not using the service;
- Prohibit Uber from tracking consumers using their device's IP address;
- Require Uber to disgorge all unlawfully obtained data;
- Limit Uber's retention of personal data;
- Compel Uber to use an automated system to monitor abuses of consumer location data; and
- Impose specific data security requirements in the comprehensive privacy program to ensure that third-party data storage services provide effective data security.

Finally, the FTC should address the risks from Uber's bug bounty program by modifying the settlement to:

[8] In the Matter of Uber Technologies, Inc., FTC File No. 152 3054 (2018) (Complaint) 6, https://www.ftc.gov/system/files/documents/cases/1523054_uber_technologies_revised_complaint_0.pdf. [hereinafter "Revised FTC Complaint"].

- Require Uber to have a non-negotiable bug bounty program that is clearly defined in company policy.

Section I of these comments sets out the procedural history of the investigation that gave rise to this Consent Order. Section II sets out EPIC's involvement and expertise in this matter. Sections III details the new allegations in the revised FTC Complaint. Section IV summarizes the changes in the modified Consent Order. Finally, Section V sets out EPIC's recommendations for how the FTC can strengthen the Consent Order to more effectively address the issues raised in the FTC's revised Complaint.

I. Procedural History

On June 22, 2015 EPIC filed a complaint with the FTC urging the Commission to investigate Uber's privacy and security practices.[9] EPIC stated that Uber's privacy policy and official statements conflicted with its business practices.[10] The complaint alleged that Uber regularly abused its access to consumer location data and failed to take adequate security measures to protect its database of sensitive user information.[11] In addition, EPIC alleged that Uber regularly abused its access to user telephone numbers and may have violated the Telephone Consumer Protection Act.[12]

Prior to Uber changing its privacy policy, EPIC had recommended privacy rules for Uber.[13] Following the disclosure of Uber's "God view" tool—which revealed that certain

[9] EPIC Uber Complaint at 3-14.
[10] *Id.* at 20.
[11] *Id.* at 21.
[12] *Id.* at 15-17.
[13] Julia Horowitz and Marc Rotenberg, *Privacy Rules for Uber,* Huffington Post, (Feb. 11, 2015) , http://www.huffingtonpost.com/julia-horwitz/privacy-rules-for-uber_b_6304824.html.

employees were tracking specific customers in Uber vehicles—EPIC recommended that clear limits be placed on employees' use of the tool.[14]

On August 15, 2017 the FTC announced a Complaint and settlement with Uber for deceiving consumers about the company's privacy and data security practices.[15] The FTC Complaint alleged that Uber had assured consumers that employee access to their personal information was closely monitored and limited. It also alleged that Uber stated that personal information provided by riders, including geolocation data, and drivers, including Social Security numbers, bank information, and insurance information, was secure in Uber databases. The FTC found, however, that Uber failed to monitor or limit employee access to customer information and failed to secure consumer data in its third-party cloud storage system—which was subject to a massive data breach in May 2014.[16]

Under the FTC's August 2017 proposed Consent Order, Uber was:

- prohibited from misrepresenting how it monitors internal access to consumers' personal information;
- prohibited from misrepresenting how it protects and secures that data;
- required to implement a comprehensive privacy program that addresses privacy risks related to new and existing products and services and protects the privacy and confidentiality of personal information collected by the company; and
- required to obtain within 180 days, and every two years after that for the next 20 years, independent, third-party audits certifying that it has a privacy program in place that meets or exceeds the requirements of the FTC order.[17]

[14] *Id*.
[15] Fed. Trade Comm'n., *Uber Settles FTC Allegations that It Made Deceptive Privacy and Data Security Claims*, Press Release, (Aug. 15, 2017), https://www.ftc.gov/news-events/press-releases/2017/08/uber-settles-ftc-allegations-it-made-deceptive-privacy-data.
[16] *Id*.
[17] In the Matter of Uber Technologies, Inc. (Decision and Order), FTC File No. 152-3054, (Aug. 15, 2017) [hereinafter "FTC Order"].

EPIC submitted extensive comments on the proposed settlement.[18] EPIC urged the Commission to strengthen the proposed settlement by limiting Uber's collection and use of consumer data, imposing specific data security requirements, and making Uber's privacy assessments available to the public. EPIC stressed that the FTC's consistent refusal to modify proposed Consent Orders in response to public comments was contrary to the FTC's statutory mission. EPIC stated that:

> [T]he Commission['s] … authority to solicit public comment is pursuant to agency regulations … A failure by the Commission to pursue modifications to proposed orders pursuant to public comment would therefore reflect a lack of diligence on the part of the Commission. If the Commission chooses not to incorporate the comments it receives on the Uber settlement, it should provide a "reasoned response." *See*, *Interstate Nat. Gas Ass'n of Am. v. F.E.R.C.*, 494 F.3d 1092, 1096 (D.C. Cir. 2007).[19]

The FTC subsequently learned in November 2017 that Uber had failed to disclose another massive data breach of its third-party cloud storage service.[20] The breach exposed unencrypted files containing more than 25 million names and email addresses, 22 million names and phone numbers, and 600,000 names and driver's license numbers.[21] Uber became aware of this breach in November 2016 but waited a full year to notify its customers while secretly paying the hackers $100,000 through its "bug bounty" program. Furthermore, Uber failed to notify the FTC of this breach despite the fact that it occurred during the FTC's investigation into Uber's failure to protect consumer data.

---

[18] Comments of EPIC, *In the Matter of Uber Technologies, Inc.*, FTC File No. 152-3054 (Sep. 15, 2017), https://epic.org/apa/comments/EPIC-FTC-Uber-Settlement.pdf.
[19] *Id*. at 4.
[20] Fed. Trade Comm'n., *Uber Agrees to Expanded Settlement with FTC Related to Privacy, Security Claims*, Press Release (Apr. 12, 2018), https://www.ftc.gov/news-events/press-releases/2018/04/uber-agrees-expanded-settlement-ftc-related-privacy-security.
[21] *Id*.

On April 12, 2018, the FTC issued a revised Complaint against Uber and announced modifications to the original settlement.[22] The modified settlement requires Uber to submit all of its biennial privacy assessments to the FTC, rather than just the initial assessment. It also imposes additional requirements in the mandated privacy program, including that Uber address: "1) secure software design, development and testing, including access key management and secure cloud storage; 2) how Uber reviews and responds to third-party security vulnerability reports, including its bug bounty program; and 3) prevention, detection and response to attacks, intrusions or failures."[23] The modified settlement also requires Uber to notify the FTC about all future incidents involving data security or face civil penalties.

II. EPIC's Involvement and Expertise

EPIC's complaint to the FTC preceded the Commission's investigation into Uber's unfair and deceptive business practices. EPIC alleged four counts that violated Section 5 of the FTC Act: (1) deceptive representation that users will be in control of their privacy settings; (2) deceptive representation that users would be able to opt-out of targeted advertising; (3) deceptive representation that users' data would be protected by robust security measures and; (4) deceptive and unfair practice of tracking users' IP addresses. To address these privacy violations, EPIC requested that the Commission:

a. Initiate an investigation of Uber's business practices, including the collection personal data from users of location data and contact list information;

b. Halt Uber's collection of user location data when it is unnecessary for the provision of the service;

[22] In the Matter of Uber Technologies, Inc. (Decision and Order), FTC File No. 152-3054, (Apr. 12, 2018) [hereinafter "Revised FTC Order"].
[23] Lesley Fair, *FTC addresses Uber's undisclosed data breach in new proposed order*, FTC Business Blog, (Apr. 12, 2018), https://www.ftc.gov/news-events/blogs/business-blog/2018/04/ftc-addresses-ubers-undisclosed-data-breach-new-proposed.

c. Halt Uber's collection of user contact list information;

d. Require the implementation of data minimization measures, including the routine deletion of location data once the ride is completed;

e. Mandate algorithmic transparency, including the publication of specific information about the rating techniques established by Uber to profile and evaluate customers;

f. Require Uber to comply with the Consumer Privacy Bill of Rights;

g. Investigate Uber's possible violation of the Telephone Consumer Protection Act;

h. Investigate other companies engaged in similar practices; and,

i. Provide such other relief as the Commission finds necessary and appropriate.[24]

III. New Allegations in the FTC's Revised Complaint

The FTC's revised Complaint alleges that in November 2016, Uber learned that intruders had gained access to consumer data stored in the Amazon S3 Datastore, Uber's third-party cloud storage service.[25] The intruders accessed the S3 Datastore using an access key that an Uber engineer had posted to GitHub, a code-sharing website used by software developers. The access key was posted in plain text format, and the intruders used that key along with passwords exposed in other large data breaches to gain access to 16 files of unencrypted personal information. These files contained approximately 25.6 million names and email addresses, 22.1 million names and mobile phone numbers, and 607,00 names and driver's license numbers.[26]

Uber failed to disclose this data breach to consumers until November 21, 2017, more than a year after discovery of the breach. When Uber discovered this data breach, it secretly paid the hackers $100,000 through a "bug bounty" program.[27] Uber maintains a bug bounty program to

[24] EPIC Uber Complaint at 22-23.
[25] Revised FTC Complaint at 5-6.
[26] *Id*.
[27] *Id*.

pay financial rewards to individuals who discover security vulnerabilities. However, these hackers were not legitimate bug bounty recipients, but were rather malicious attackers who exploited Uber's security vulnerabilities to acquire personal information on millions of consumers in exchange for a ransom. Furthermore, Uber did not disclose this data breach to the FTC despite the fact that it occurred during the FTC's investigation into Uber's 2014 data breach, which was also the result of Uber's data security failures.

The FTC found that Uber violated Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45(a), by representing to consumers that it provided reasonable data security for personal information stored in its databases.[28] As the new allegations make clear, Uber failed to provide reasonable data security and therefore the representations made to consumers were false or misleading.

IV. The Revised FTC Settlement

Part I – Prohibition Against Misrepresentation

Uber is prohibited from misrepresenting "the extent to which [Uber] monitors or audits internal access to consumers' Personal Information" and "the extent to which [Uber] protects the privacy, confidentiality, security, or integrity of any Personal Information."[29] This part is identical to the August 2017 proposed consent agreement.

Part II – Mandated Privacy Program

Uber must implement and maintain "a comprehensive privacy program that is reasonably designed to (1) address privacy risks related to the development and management of new and

[28] *Id*.
[29] Revised FTC Order at 2.

existing products and services for consumers, and (2) protect the privacy and confidentiality of Personal Information."[30]

Part II.B has been revised to require Uber to address the privacy and data security risks specifically 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.[31]

Part III – Privacy Assessments by a Third Party

Uber must undergo biennial privacy assessments every two years. These assessments "must be completed by a qualified, objective, independent third-party professional" and occur every two years for the next 20 years.[32] Each assessment must detail specific privacy controls that Uber has put in place, explain how the privacy controls are appropriate given Uber's size, nature and scope of their activities, and sensitivity of the information being stored, explain how the privacy controls being used meet or exceed the provisions of the FTC Order, and certify that privacy controls are operating effectively and provide reasonable assurances that the privacy of consumer information will be protected.[33]

Part III has been revised to require Uber to submit each of its biennial privacy assessments to the FTC, rather than only the initial assessment.

Parts IV – Covered Incident Reports

Uber must submit a report to the FTC if it discovers any "covered incident" involving unauthorized access or acquisition of consumer information. This report must include: 1) the date

[30] *Id*. at 3.
[31] *Id*.
[32] *Id.*
[33] *Id.* at 4.

and time of the incident; 2) a description of the incident; 3) a description of each type of information that triggered the notification obligations; 4) the number of affected consumers; 5) the steps Uber has taken to remediate the incident; and 6) a copy of each notice of the incident required by law.[34] This part is new.

Parts V - IX – Reporting and Compliance

The revised Order contains enhanced reporting and compliance provisions. Part V requires Uber to obtain signed acknowledgements of the order from all employees, agents, and representatives who regularly access personal information that Uber collects. Part VII contains modified recordkeeping provisions related to Uber's bug bounty program. It requires Uber to retain records "from individuals or entities that seek payment, rewards, or recognition through a 'bug bounty' or similar program for reporting a security vulnerability." It also requires Uber to retain copies of all subpoenas and communications with law enforcement.[35]

V. EPIC's Assessment of the Modified Order and Recommendations

EPIC supports the modifications to the FTC's proposed Consent Order. These modifications make clear that companies will face enhanced penalties if they continue to misrepresent their business practices during an FTC investigation. The modifications also address some of the concerns EPIC raised in its initial comments in response to the August 2017 proposed settlement. In particular, the modified settlement requires Uber to notify the FTC of all future data breaches, to submit each of its biennial privacy assessments to the FTC, and to retain records related to its bug bounty program. The modified order also enhances the requirements in the comprehensive privacy program by requiring Uber to identify specific risks related to its third-party data storage.

[34] *Id*. at 5.
[35] *Id*. at 5-7.

However, the modified order still falls short in significant ways. The Order fails address numerous issues that EPIC raised in previous comments and fails to adopt any of EPIC's recommendations. Therefore, EPIC again puts forth the following recommendations for how the FTC can strengthen the proposed order. In addition to EPIC's previous recommendations, the FTC should also require Uber to have a non-negotiable bug bounty program that is clearly defined in company policy.

1. Require Uber's Privacy Assessments to be Made Available to the Public

To assure compliance with the FTC Order, Uber must undergo privacy assessments every two years and submit them to the Commission.[36] While the modified Order requires Uber to submit all of its assessments to the FTC, rather than only the first assessment, it does not require that these privacy assessments be made public. The recent allegations have cast serious doubt on whether the public can trust Uber's representations regarding its data security practices. Releasing the mandated privacy assessments is the only way to allow consumers to determine whether they can safely and securely continue to use Uber's services. Consumers cannot be sure that Uber is taking its obligations under the Consent Order seriously unless the FTC makes Uber's biennial privacy assessments available to the public.

As the FTC stated in its revised Complaint, Uber failed to disclose its November 2016 data breach for over a year while it was under investigation for previous data security failures.[37] The November 2016 breach exposed personal information stored in Uber's Amazon S3 Datastore—the very database which Uber failed to safeguard in 2014, resulting in a similar data breach. The FTC found in its initial complaint that in 2014 Uber had failed to implement reasonable access controls to prevent unauthorized access to data stored in the Amazon S3

[36] Revised FTC Order at 3-4.
[37] Revised FTC Complaint at 5-6.

Datastore.[38] Uber allowed all programs and engineers to use a single access key to gain access to sensitive personal information stored in plain, unencrypted text.[39] In May 2014, Uber suffered a data breach as a result of this failure, in which an intruder was able to access unencrypted personal information using a publicly available access key that provided full administrative privileges to the S3 Datastore.[40] While the FTC was investigating this breach, Uber became aware of another data breach in November 2016 that once again exposed unencrypted personal information stored in the S3 Datastore.[41] Uber willfully concealed this breach from both the FTC and the public during the FTC's investigation. Uber did not disclose this data breach until November 2017, more than a year after it discovered the breach and a full three months after the FTC charged Uber with misleading consumers regarding its data security practices.[42]

In addition, Uber has repeatedly issued false and misleading statements regarding how it monitored employee access to such personal information. In November 2014, Uber stated that it closely monitored and audited its employees' access to consumer accounts.[43] Uber further stated that it had developed an automated system for monitoring access to consumer personal information.[44] But the FTC found that Uber's automated system was not designed or staffed to effectively handle ongoing review of access to data by Uber's thousands of employees and contingent workers.[45] The FTC further found that Uber failed to follow up on alerts regarding the

[38] *Id*. at 5.
[39] *Id*.
[40] *Id*.
[41] *Id*.
[42] *Id*. at 6.
[43] *Id*. at 4.
[44] *Id*.
[45] *Id*.

misuse of consumer information and only monitored access to account information belonging to a set of internal high-profile users, such as Uber executives.[46]

Uber also has a history of taking steps to evade regulators and law enforcement. In March of 2017, it was widely reported that Uber had taken steps to avoid law enforcement through its "Greyball" tool.[47] This program utilized geolocation data, credit card information, and social media accounts to identify individuals working for local government agencies in areas where Uber's services were currently being resisted by local governments or had been banned. This program would show individuals suspected of working for local governments where cars were, but no driver would respond to their request to be picked up. Uber employees who confirmed the existence of Greyball did so anonymously for fear of being retaliated against by Uber.[48] The use of Greyball is currently the subject of a federal inquiry by the Department of Justice.[49] Uber has also sought to slight regulators in connection with its self-driving car program. The California Department of Motor Vehicles ordered Uber to end its self-driving car program, which was testing the experimental vehicles in San Francisco, after determining the program was not in compliance with state rules.[50] Despite these demands, Uber has continued its self-driving car program, which last month resulted in a fatal accident in Arizona.[51]

---

[46] *Id*.
[47] Julia Carrie Wong, *Greyball: How Uber Used Secret Software To Dodge The Law,* The Guardian, (Mar. 3, 2017), https://www.theguardian.com/technology/2017/mar/03/uber-secret-program-greyball-resignation-ed-baker.
[48] Mike Isaac, *How Uber Deceives the Authorities Worldwide,* New York Times, (Mar. 3, 2017), https://www.nytimes.com/2017/03/03/technology/uber-greyball-program-evade-authorities.html.
[49] Mike Isaac, *Uber Faces Federal Inquiry Over Use Of Greyball Tool to Evade Authorities,* (May 4, 2017), https://www.nytimes.com/2017/05/04/technology/uber-federal-inquiry-software-greyball.html.
[50] David Pierson, *Uber Defies DMV's Order To Cease Self-Driving Car Program In San Francisco,* Los Angeles Times, Dec. 16, 2016, http://www.latimes.com/business/la-fi-tn-uber-20161216-story.html.
[51] Daisuke Wakabayashi, *Self-Driving Uber Car Kills Pedestrian in Arizona, Where Robots Roam*, NY Times, (Mar. 19, 2018), https://www.nytimes.com/2018/03/19/technology/uber-driverless-fatality.html.

To hold Uber accountable to the public, the FTC must make Uber's biennial privacy assessments publicly available.

2. Require Uber to Provide Consumers with Access to the Personal Data Maintained by Uber

EPIC supports the provisions in Section I of the proposed Order prohibiting Uber from making any misrepresentations about the extent to which the company monitors its employees' access to consumers' personal information, or the extent to which the company protects consumers' privacy.[52] EPIC also supports the provisions in Section III requiring Uber to submit biennial privacy audits to the FTC.[53] Nonetheless, the proposed Order fails to address the range of problems identified by EPIC, the ongoing practices of Uber that threaten consumer privacy, or to provide adequate assurances that similar privacy violations will not occur in the future.

The Commission should strengthen the proposed Order by requiring Uber to provide consumers with access to the personal data maintained by Uber. Consumers should have a method to find out what information about them Uber has and how it is being used, in accordance with the principles set out in the Code of Fair Information Practices.[54]

3. Prohibit Uber From Tracking Consumers and Accessing Contact Lists When They Are Not Using the Service

Uber recently announced that it would end its practice of tracking consumers before and after rides.[55] However, the FTC should bind Uber to its public commitment to stop tracking consumers when they are not using the app. According to Uber's revised, 2015 privacy policy,

---

[52] Revised FTC Order at 2.
[53] *Id*. at 3-4.
[54] *See* EPIC, *The Code of Fair Information Practices,* https://epic.org/privacy/consumer/code_fair_info.html.
[55] Dustin Volz, *Uber To End Post-Trip Tracking Of Riders As Part Of Privacy Push,* Reuters, Aug. 29, 2017, https://www.reuters.com/article/us-uber-privacy/uber-to-end-post-trip-tracking-of-riders-as-part-of-privacy-push-idUSKCN1B90EN.

Uber was collecting geolocation data of consumers "when the app is running in the foreground or background."[56] Although iOS users had the ability to disable this feature by changing their settings, Android users had no way of preventing Uber from collecting their geolocation data.[57] Moreover, not only did many consumers not have the option of preventing Uber from collecting geolocation data when they were not using the app, but even if consumers disabled GPS location services on their phone entirely, Uber was still able to derive their approximate location from their phone's IP address.[58]

Uber has never explained why access to a consumer's location when the app is turned off or to a consumer's contact list was necessary to use the service. Uber has claimed that it will use this data for purposes other than ride-sharing, such as "facilitating social interactions" or "allow[ing] Uber to launch new promotional features."[59] This is an unfair business practice because the invasion of consumers' privacy is not offset by any benefit to consumers, and there is clearly no way for consumers to avoid the harm if they have no ability to prevent Uber from collecting this data.[60]

To help restore public trust in Uber, the FTC should require Uber to cease tracking consumers and accessing contact lists when they are not using the service.

4. <u>Prohibit Uber From Tracking Consumers Using Their Device's IP Address</u>

---

[56] Uber Privacy Policy, https://www.uber.com/legal/privacy/users/en/.
[57] Sunainaa Chadha, *If You Have An Android Phone, Uber's New Privacy Policy Will Spook You*, firstpost.com, May 29, 2015, http://www.firstpost.com/business/android-phone-ubers-new-privacy-policy-will-spook-2269042.html.
[58] John Ribeiro, Uber Revises Privacy Policy, Wants More Data From Users, networkworld.com, May 28, 2015, https://www.networkworld.com/article/2928513/uber-revises-privacy-policy-wants-more-data-from-users.html.
[59] Dara Kerr, Uber Updates Privacy Policy, But Can Still Track Users, CNET, May 29, 2015, http://www.cnet.com/news/uber-updates-privacy-policy-but-can-still-track-users/
[60] Fed. Trade Comm'n, FTC Policy Statement on Unfairness (1980), http://www.ftc.gov/bcp/policystmt/ad-unfair.htm.

The Commission should prohibit Uber from using a consumer's IP address to track their proximate location. EPIC alleged in its complaint to the FTC that this constitutes an unfair business practice because it is likely to cause substantial injury to consumers, which is not reasonably avoidable by consumers themselves and is not outweighed by countervailing benefits to consumers or to competition.[61] The injury is substantial because deriving users' proximate locations without their knowledge poses potential safety risks. Uber's IP tracking undermines consumers' decision-making autonomy when they expressly decline to disclose their location data to Uber. This injury is not reasonably avoidable by consumers themselves because they must completely delete the app or cease using Uber's services to stop Uber from collecting their IP addresses. Furthermore, Uber has not presented any legitimate business purpose or substantial benefit to consumers derived from IP tracking.

5. Require Uber to Disgorge All Unlawfully Obtained Data

The FTC Order is purely prospective and does not attempt to reverse or negate the unfair and deceptive business practices that resulted in the Complaint and Order. As the harm arose from Uber's unfair and deceptive practices regarding its collection of consumers' personal information, equitable relief requires the Commission to mandate that Uber disgorge all personal data that it obtained unlawfully.

6. Limit Uber's Retention of Personal Data

Uber has not established a legitimate business justification for keeping much of the personal data it collects. While storing certain information, such as payment information and a consumer's home address, may serve a legitimate purpose for using the app, there is no

[61] EPIC Uber Complaint at 22.

legitimate justification for Uber to store trip information for every ride or to retain that data after the service is provided.

7. Compel Uber to Use an Automated System to Monitor Abuses of Consumer Location Data

The FTC's privacy program should prevent further abuses of customer location data by Uber employees. Abuses of the "God View" tool that allowed Uber employees to view an individual user's real-time and historic geolocation data were among the most alarming allegations in the complaint. However, the proposed Order does not specifically address the privacy concerns unique to this feature.

After considerable public outrage following revelation of employee misuse of this tool, Uber issued a statement reassuring consumers that it created a new "strict policy prohibiting all employees at every level from accessing a rider or driver's data" except for a "limited set of legitimate business purposes."[62] Uber claimed that access to rider and driver information would be closely monitored and that violations of the policy would result in disciplinary action.[63] As detailed in the FTC's complaint, Uber did not honor its promises and failed to respond to alerts of potential misuse in a timely manner and only monitored access for a small number of employees.[64] While voluntary measures taken by Uber are welcome, Uber's poor track record of abiding by its own privacy policies demonstrate that the FTC should set more stringent requirements for the company to meet.

The FTC's privacy program should require Uber to routinely monitor employee access to consumer data. Audit software can monitor employee access to sensitive information and send alerts when a use is voyeuristic or otherwise inappropriate. This will result in records of when

[62] FTC Complaint at 2.
[63] *Id.*
[64] *Id.* at 3

employees access personal information that can be consulted if there is a question as to whether the employee's access was for a legitimate business purpose. Uber created and used an automated system for several months but failed to adequately monitor and review information provided by the system and later abandoned its use. Once it was abandoned, only high-profile Uber employees were monitored unless an employee was reported by a coworker.[65] The FTC should require Uber to implement an automated system that reports inappropriate access and use of consumer information and require that the system be adequately staffed, monitored, and reviewed to detect any inappropriate access.

8. Impose Specific Data Security Requirements in the Comprehensive Privacy Program to Ensure That Third-Party Data Storage Services Provide Effective Data Security

EPIC supports the modifications to the proposed order that enhance the requirements of Uber's comprehensive privacy program. Under the modified order, Uber must address specific risks related to its third-party data storage service and its bug bounty program. The FTC should go a step further, however, and impose specific data security requirements to ensure that Uber does not continue allow unauthorized access to personal data stored in its third-party data storage service.

The FTC's revised complaint details how Uber has now twice allowed hackers to access sensitive consumer data as a result of its failure to implement reasonable access controls to safeguard the data stored in its Amazon S3 Datastore. According to the FTC's original complaint, Uber compromised consumer data by "failing to require programs and engineers that access the Amazon S3 Datastore to use distinct access keys," and by "failing to require multi-factor authentication for access to the Amazon S3 Datastore."[66]

[65] *Id.*
[66] FTC Complaint at 4.

On May 12, 2014, this storage service was subject to a security breach, as an intruder was able to gain access to all the data and documents stored within this database by using a single access key that one of Uber's engineers had publicly posted online.[67] This intruder was able to gain access to unencrypted bank account numbers, Social Security Numbers, names, addresses, and stored location information. Uber did not discover this breach until September 2014. Cybersecurity experts have described this massive trove of personal information as a "sitting duck" for hackers.[68]

On November 14, 2016, this storage service was subject to a second security breach; intruders once again used publicly posted access keys to gain access to unencrypted files containing the personal information of millions of Uber riders and drivers.

Despite Uber's repeated failures to protect consumer data, the proposed Order contains no mandatory provisions for how Uber will safeguard consumer data. The revised settlement simply requires Uber to "address privacy risks" related to several aspects of its third-party data storage.[69] The FTC should require Uber to prevent full access to its third-party storage system using one single access key. The FTC should also mandate that Uber's third-party storage system employ multiple levels of encryption and anonymization to ensure that sensitive information is not stored in easily-readable plain text files.

9. <u>Require Uber to Have a Non-negotiable Bug Bounty Program That Is Clearly Defined in Company Policy.</u>

[67] Tracey Lien, *Uber Security Breach May Have Affected Up to 50,000 Drivers*, Los Angeles Times, Feb. 27, 2015, http://www.latimes.com/business/technology/la-fi-tn-uber-data-breach-20150227-story.html.
[68] Craig Timberg, *Is Uber's Rider Database a Sitting Duck for Hackers?,* Washington Post, (Dec. 1, 2014), http://www.washingtonpost.com/blogs/the-switch/wp/2014/12/01/is-ubers-rider-database-a-sitting-duck- for-hackers/.
[69] Revised FTC Order at 4.

EPIC supports the additional provisions in the modified order that require Uber to assess risks and retain records related to its bug bounty program. But the modified order should impose specific requirements for a bug bounty program to prevent Uber's abuse of such program. Bug bounty programs serve legitimate purposes in both the public and private sector. They allow white hat hackers to disclose security vulnerabilities in an ethical way. But Uber used its bug bounty program to mislead the public and cover up a data breach. Joe Sullivan, Uber's chief security officer (who has since been fired) denied that the November 2016 incident was a breach and said the company had treated it as an authorized vulnerability disclosure.[70] But emails between Uber and the hacker revealed more complicated circumstances. After Uber told the hacker that the max payout of their bug bounty program was $10,000, the hacker responded that he expected at least $100,000 and then threatened the company.[71]

Bug bounties need to be non-negotiable and clearly defined in company policy; otherwise, companies are letting user data be held as ransom. $100,000 could have been an appropriate bounty for Uber to pay. In January 2018, Google paid a security researcher $112,500 for an Android bug,[72] and Apple offers up to $200,000 for iOS and iCloud bugs.[73] But the communications between Uber and the hacker make the $100,000 payment look more like extortion than a payment for services.

---

[70] Nicole Perlroth and Mike Isaac, *Inside Uber's $100,000 Payment to a Hacker, and the Fallout*, N.Y. Times (Jan. 12, 2018), https://www.nytimes.com/2018/01/12/technology/uber-hacker-payment-100000.html?_r=0.

[71] *Id.* (One email read: "Yes we expect at least 100,000$ I am sure you understand what this could've turned out to be if it was to get in the wrong hands, I mean you guys had private keys, private data stored, backups of everything, config files etc... This would've heart [sic] the company a lot more than you think.")

[72] Charlie Osborne, *Google awards researcher over $110,000 for Android exploit chain*, ZDNet (Jan. 18, 2018), http://www.zdnet.com/article/google-awards-researcher-over-110000-for-android-exploit-chain/.

[73] Andrew Cunningham, *Starting this fall, Apple will pay up to $200,000 for iOS and iCloud bugs*, ArsTechnica (Aug. 4, 2016), https://arstechnica.com/gadgets/2016/08/starting-this-fall-apple-will-pay-up-to-200000-for-ios-and-icloud-bugs/.

Conclusion

EPIC supports the FTC's decision to modify the proposed Consent Order in response to Uber's continued failure to protect consumer privacy and data security. But there is much more that needs to be done to address the consumer privacy concerns arising from Uber's business practices. Specifically, EPIC urges the Commission to make all of Uber's privacy assessments available to the public. EPIC reminds the FTC that the Commission is required by statute to meaningfully consider comments submitted by the public before finalizing consent orders, and to provide a reasoned response to such comments. Most importantly, it is the responsibility of the FTC to protect consumer privacy and prosecute companies that engage in unfair and deceptive trade practices.

Respectfully submitted,

/s/ Marc Rotenberg
Marc Rotenberg
EPIC President

/s/ Sam Lester
Sam Lester
EPIC Consumer Privacy Counsel

/s/ Christine Bannan
Christine Bannan
EPIC Policy Counsel