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

September 15, 2017

By notice published on August 21, 2017, the Federal Trade Commission ("FTC") has proposed a consent agreement with Uber Technologies, Inc. that would settle "alleged violations of federal law prohibiting unfair or deceptive acts or practices."[1] The Consent Order ("Order") follows the FTC's Complaint, which 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," and that "Uber failed to provide reasonable security for consumer information stored in a third-party cloud storage service."[2]

These comments on the FTC's proposed Order are submitted on behalf of the Electronic Privacy Information Center ("EPIC"), a public interest research center in Washington, D.C. EPIC was established in 1994 to focus public attention on emerging civil liberties issues and to

[1] Uber Technologies, Inc; Analysis of to Aid Public Comment, 82 Fed. Reg. 39,582 (August 21, 2017).
[2] *Id*.

protect privacy, the First Amendment, and constitutional values. EPIC has a particular interest in protecting consumer privacy, and 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.[3] EPIC filed a complaint with the FTC alleging many of the same harms identified by the FTC.[4] EPIC routinely files complaints with the FTC alerting the agency to practices that harm consumer privacy.[5]

EPIC supports the findings in the FTC Complaint and many of the directives contained in the Order. The Complaint makes clear that companies should not engage in unfair and deceptive trade practices, particularly in the collection and use of personal data. In such circumstances, the FTC has the authority and the obligation to act to protect the interests of consumers. The

---

[3] 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 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, Request for Investigation and for Other Relief, before the Federal Trade Commission (Dec. 16, 2004), available at http://epic.org/privacy/choicepoint/fcraltr12.16.04.html.

[4] 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"].

[5] 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.

proposed Order that follows from the Complaint outlines several measures to safeguard the interests of consumers.

To further protect the interests of consumers and to make clear the full scope of a Comprehensive Privacy Program that is mandated for Uber, EPIC recommends that the FTC:

- Require Uber to provide customers access to personal data maintained by Uber;
- Prohibit Uber from tracking customers and accessing contact lists when they are not using the service;
- Prohibit Uber from tracking consumers using their phone'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 customer location data;
- Impose specific requirement in the comprehensive privacy program to ensure that third party data storage services provide effective data security; and
- Require that Uber's privacy assessments are made available to the public.

EPIC has previously submitted comments to the Commission on numerous proposed orders that implicate the privacy interests of consumers.[6] However, to date the Commission has adopted these consent orders without any modification. Nonetheless, EPIC offers these recommendations to strengthen the proposed settlement and to protect the interests of consumers.

[6] Comments of EPIC, *In the Matter of Snapchat, Inc.,* FTC File No. 132 3078, Jun. 9, 2014, https://epic.org/apa/comments/FTC-Snapchat-Cmts.pdf; Comments of EPIC, *In the Matter of Myspace LLC,* FTC Docket No. 102 3058, Jun. 8, 2012, https://epic.org/privacy/socialnet/EPIC-Myspace-comments-FINAL.pdf; Comments of EPIC, *In the Matter of Facebook, Inc.* FTC Docket No. 092 3184, Dec. 27, 2011, https://epic.org/privacy/facebook/Facebook-FTC-Settlement-Comments-FINAL.pdf; Comments of the EPIC, *In the Matter of Google,* FTC Docket No. 102 3136, May 2, 2011, https://epic.org/privacy/ftc/googlebuzz/EPIC_Comments_to_FTC_Google_Buzz.pdf.

EPIC reminds the Commission that its authority to solicit public comment is pursuant to agency regulations. Commission Rules of Practice, 16 C.F.R. § 2.34 states:

> **(c) Public comment.** Promptly after its acceptance of the consent agreement, the Commission will place the order contained in the consent agreement, the complaint, and the consent agreement on the public record for a period of 30 days, or such other period as the Commission may specify, for the receipt of comments or views from any interested person.
>
> **(e) Action following comment period.**
> **(2**) The Commission, following the comment period, may determine, on the basis of the comments or otherwise, that a Final Decision and Order that was issued in advance of the comment period should be modified. Absent agreement by respondents to the modifications, the Commission may initiate a proceeding to reopen and modify the decision and order in accordance with § 3.72(b) of this chapter or commence a new administrative proceeding by issuing a complaint in accordance with § 3.11 of this chapter.

The provision allows private parties to withdraw from proposed consent orders. As one court has explained, "[s]ince the Commission can withdraw its acceptance, two contract principles permit consent order respondents to withdraw their consent so long as the withdrawal occurs prior to a final decision by the Commission" *Johnson Prod. Co. v. F.T.C., 549 F.2d 35, 37 (7th Cir. 1978).*

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).*

Section I sets out the procedural history of the investigation concerning the business practices that gave rise to this Consent Order. Section II sets out EPIC's involvement and expertise in this matter. Sections III and IV detail the FTC Complaint and summarize the FTC

Consent Order. Section V sets out EPIC's comments and recommendations regarding the Consent Order that would strengthen privacy protections and more effectively address the issues raised in the Complaint.

I. Procedural History

On May 28, 2015 Uber revised its "Privacy Policy" and claimed that "users will be in control: they will be able to choose whether to share the data with Uber."[7]

On June 22, 2015 EPIC filed a complaint with the FTC urging the Commission to investigate Uber's privacy and security practices.[8] EPIC stated that Uber's privacy policy and official statements conflicted with its business practices.[9] The complaint alleged that Uber regularly abused its access to customer location data and failed to take adequate security measures to protect its database of sensitive user information.[10] Additionally, it alleged Uber regularly abused its access to user telephone numbers and may have violated the Telephone Consumer Protection Act.[11] Furthermore, prior to Uber changing its privacy policy, EPIC recommended privacy rules for Uber.[12] Specifically, following the disclosure of Uber's "God view" tool, which revealed that certain employees were tracking specific customers in Uber vehicles, EPIC recommended that clear limits be placed on employees use of the tool.

On August 15, 2017 the FTC announced that it had issued a complaint against, and subsequently settled with, Uber for false and misleading statements concerning the privacy and

---

[7] Katherine Tassi, *An Update On Privacy at Uber*, Uber, May 28, 2015, http://newsroom.uber.com/2015/05/an-update-on-privacy-at-uber/

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

data security practices.[13] The FTC complaint highlighted representations that Uber had made to driver and riders concerning their privacy and security practices. Uber assured consumers that personal information was closely monitored and access to that information was limited. Uber also 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.

According to the FTC, "[u]nder its agreement with the Commission, Uber is:

- "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."[14]

In the announcement of the proposed settlement, FTC Acting Chairman Maureen Ohlhausen stated that "Uber failed consumers in two key ways: First by misrepresenting the

[13] *Uber Settles FTC Allegations That It Made Deceptive Privacy and Data Security Claims,* Federal Trade Commission, Aug. 15, 2017, https://www.ftc.gov/news-events/press-releases/2017/08/uber-settles-ftc-allegations-it-made-deceptive-privacy-data.
[14] In the Matter of Uber Technologies, Inc. (Decision and Order), Federal Trade Commission, Aug. 15, 2017 [hereinafter "FTC Order"].

extent to which it monitored its employees' access to personal information about users and drivers, and second by misrepresenting that it took reasonable steps to secure that data."[15]

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;
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;

[15] *Uber Settles FTC Allegations That It Made Deceptive Privacy and Data Security Claims,* Federal Trade Commission, Aug. 15, 2017, https://www.ftc.gov/news-events/press-releases/2017/08/uber-settles-ftc-allegations-it-made-deceptive-privacy-data.

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

i. Provide such other relief as the Commission finds necessary and appropriate. [16]

III. FTC Complaint Allegations

The FTC's Complaint addressed several of the issues set out in the EPIC filing. The FTC Complaint explained that Uber is an App that collects substantial personal information from Uber drivers and riders.[17] Specifically, the FTC states that Uber obtains a drivers name, e-mail address, Social Security number, drivers license information, insurance information, and bank account information.[18] Uber also collects personal information from riders including names, e-mail addresses, and trip records with precise geolocation information.[19] The FTC Complaint also states that in December 2015 riders had completed more than 1 billion rides using the Uber App.[20]

The FTC Complaint described internal access to rider and driver personal information as well as Uber's security practices. The FTC found that Uber had allowed employees to improperly access customer information, including location data, and wanted to use that information to look into the personal lives of journalists who criticized Uber's business practices.[21] The FTC also described Uber's "God View" tool which displayed personal information of riders using Uber.[22] Following public reports of this misuse of consumer data, Uber stated that they would closely monitor and audit their employees access to rider and driver

[16] EPIC Uber Complaint at 22-23.
[17] In the Matter of Uber Technologies Inc. (Complaint), Federal Trade Commission [hereinafter "FTC Complaint"].
[18] FTC Complaint at 2.
[19] *Id.*
[20] *Id.*
[21] *Id.*
[22] *Id.*

accounts.[23] However, the FTC then discusses how Uber failed to undergo close monitoring, instead choosing to use an automated system to monitor employee access to personal information and failed to adequately staff that system to allow for ongoing review to determine how data was accessed.[24] The FTC also reported that Uber failed to respond to alerts about the potential misuse of consumer information and only monitored access to internal high-profiles users, such as Uber executives.[25] During development of the new system, Uber also failed to monitor internal access to personal information unless an Uber employee specifically reported that a co-worker had inappropriately accessed information.[26]

The FTC also discussed Uber's data storage practices. The FTC stated that for two years Uber's privacy policy stated that Uber was taking steps to protect personal information that it collected from consumers and customer service representatives repeatedly assured consumers that the personal information they provided to Uber was safe.[27] The FTC concluded that those statements were misleading. The FTC said that Uber failed to take reasonable steps that would have prevented access to consumer information that was stored in a cloud service operated by Amazon. Specifically, the FTC found that Uber failed to take reasonable measures such as limiting who had access to data, implementing security training and guidance, having a written information security program, and failed to encrypt sensitive information.[28] The FTC explained that Uber's practices "created serious risks for consumers" and that as a result of Uber's lax security practices Uber suffered a data breach.[29] The data breach was the result of an engineer

[23] *Id.*
[24] *Id.* at 3.
[25] *Id.*
[26] *Id.*
[27] *Id.* at 4.
[28] *Id.* at 5.
[29] *Id.*

that had publicly posted an access to key on a code-sharing website allowing an intruder to access a single file that contained sensitive personal information including unencrypted names, drivers license numbers, bank accounts, and Social Security numbers.[30] This breach affected thousands Uber Drivers who were not promptly notified of the data breach.[31]

Section 5 Violations

The FTC found the Uber had committed two Section 5 violations. First, Uber's representations that consumers personal information was closely monitored and audits was false or misleading as demonstrated by Uber's use of an automated system that they routinely failed to monitor.[32] Second, Uber representations that they took reasonable security measures to protect consumer personal information were false and misleading as demonstrated by Uber's failure to take reasonable security measures and the subsequent data breach that exposed the personal information of thousands of Uber drivers.[33]

IV. 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."[34]

Part II – Mandated Privacy Program

---

[30] *Id.*
[31] *Id.*; Dave Lewis, *Uber Suffers Data Breach Affecting 50,000,* Forbes, Feb. 28, 2015, https://www.forbes.com/sites/davelewis/2015/02/28/uber-suffers-data-breach-affecting-50000/#31f202942db1.
[32] FTC Complaint at 5.
[33] *Id.* at 6.
[34] FTC Order at 2.

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 existing products and services for consumers, and (2) protect the privacy and confidentiality of Personal Information."[35] The program "must contain controls and procedures appropriate to [Uber's] size and complexity, the nature and scope of [Uber's] activities, and the sensitivity of the Personal Information."[36] The program must include an employee(s) that will coordinate and be responsible for the program, identify reasonably foreseeable internal and external risks that could result in the unauthorized collection, use, and disclosure of personal information, assess whether safeguards being used to guard sensitive information are sufficient, design and implement controls and procedures to address security risks, develop and use reasonable steps to select and retain service providers to assist in protecting personal information, and evaluate and adjust the privacy program as the result of routine tests and monitoring that Uber will conduct.[37]

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. [38] 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 provision's of the FTC Order, and certify that

[35] FTC Order at 2.
[36] *Id* at 3.
[37] *Id*.
[38] *Id.*

privacy controls are operating effectively and provide reasonable assurances that the privacy of consumer information will be protected.[39]

Parts IV – VIII – Additional Requirements

Uber must also submit to the FTC "an acknowledgement of receipt of [the] Order" and deliver copies of the order to "(1) all principals, officers, directors, and LLC managers and members; (2) all employees, agents, and representatives having managerial responsibility for conduct related to the subject matter of the order; and (3) any business entity resulting from any change in structure as set forth in the Provision of this Order."[40] Uber must provide signed and dated acknowledgement of receipts for all persons and entities who receive a copy of the Order.

Uber also must submit compliance reports to the FTC.[41] These reports must identify physical, postal, and e-mail addresses for Uber and its subsidiaries, discuss how Uber and its subsidiaries are in compliance with the Order, what changes have been made to come into compliance with the Order, and notice for the filing of any bankruptcy petition, insolvency proceeding, or similar proceeding by or against Uber.

Uber must create records for 20 years and retain those records for 5 years unless otherwise specified.[42] These records include accounting records, personnel records, records of all consumer complaints directed at or forwarded to Uber, records necessary to demonstrate compliance with the Order, and copies of widely disseminated representations by Uber that describe how it maintains or protects privacy, security, and confidentiality of personal information.

---

[39] *Id.*
[40] *Id.* at 4.
[41] *Id.* at 5.
[42] *Id.* at 6.

To allow for accurate monitoring and to determine compliance with the Order, Uber also must submit additional compliance reports or other requested information within 10 days of receipt of a written request from a representative of the FTC.[43]

V. Recommendations

Under the proposed Order with the FTC, Uber has agreed to cease making false or misleading statements; implement a comprehensive privacy program that (1) addresses 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; and (3) undergo privacy assessments to be conducted by an independent third-party. Consistent with those objectives, EPIC makes the following recommendations:

(1) Require Uber To Provide Customers Access To 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 regarding the extent to which the company protects consumers' privacy. EPIC also supports the Commission's determinations in Section III requiring Uber to submit to biennial privacy audits. 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 and require Uber to provide customers with access to the personal data maintained by Uber. Consumers should have a

[43] *Id*.

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 [44]

Recommendation: The Commission should require Uber to grant customers access to all personal data it maintains on them.

(2) Prohibit Uber From Tracking Customers And Accessing Contact Lists When They Are Not Using The Service

The FTC should prohibit Uber from accessing customers contact lists and geolocation data when they are not using the service. The FTC has repeatedly emphasized the importance of consumer control over their information[45] and EPIC agrees that user control is the cornerstone of consumer privacy. For instance, in the recent Lenovo consent order the Commission required that Lenovo obtain consumers' affirmative consent before it pre-installed software on their computers.[46]

Uber recently announced that it would end its practice of tracking consumers before and after rides.[47] However, the FTC should revise this Order to bind Uber to its public commitment to stop tracking consumers when they are not using the app. According to Uber's revised, 2015

[44] *See* EPIC, *The Code of Fair Information Practices,* https://epic.org/privacy/consumer/code_fair_info.html. [hereinafter "Fair Information Practices"]
[45] *See*, *e.g.* FTC Report: Protecting Consumer Privacy In An Era Of Rapid Change, https://www.ftc.gov/news-events/press-releases/2012/03/ftc-issues-final-commission-report-protecting-consumer-privacy; FTC Recommends Congress Require the Data Broker Industry to be More Transparent and Give Consumers Greater Control Over Their Personal Information, *available at* https://www.ftc.gov/news-events/press-releases/2014/05/ftc-recommends-congress-require-data-broker-industry-be-more.
[46] In the Matter of Lenovo, File No. 152 3134 (Agreement Containing Consent Order), Federal Trade Commission.
[47] 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.

privacy policy, Uber was collecting geolocation data of consumers "when the app is running in the foreground or background."[48] 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.[49] Moreover, not only did many consumers not have the option of preventing Uber from collecting geolocation data when they were not using the app, 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.[50] The FTC took great lengths to discuss Uber's past history of making misleading statements in its complaint.[51] To help restore public trust in Uber, the FTC should bind Uber to its publicly stated, voluntary action to end this practice.

Uber never explained why access to a consumer's location when the app is turned off is 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."[52] 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 tracking them.[53]

---

[48] Uber Privacy Policy, https://www.uber.com/legal/privacy/users/en/.
[49] 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.
[50] 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.
[51] *See generally,* FTC Complaint.
[52] 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/
[53] Fed. Trade Comm'n, FTC Policy Statement on Unfairness (1980), http://www.ftc.gov/bcp/policystmt/ad-unfair.htm.

Recommendation: The Commission should prohibit Uber access to customers contacts and end the tracking of customers when they are not using the service.

(3) Prohibit Uber From Tracking Consumers Using Their Phone's IP Address

The Commission should also prohibit Uber from using a consumer's IP address to track his or her proximate location. As mentioned above, Uber tracks its users through their phone's IP addresses, and as EPIC stated in its complaint to the FTC, 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.[54] 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 evidence of a legitimate business purpose or a substantial benefit to consumers served by IP tracking.

Recommendation: The Commission should amend the proposed Order to prohibit Uber from tracking consumers by using their phones' IP addresses.

(4) Require Uber To Disgorge All Unlawfully Obtained Data

[54] EPIC Uber Complaint at 22.

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.

Recommendation: The Commission should require Uber to delete all personal data it obtained unlawfully.

(5) 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 legitimate justification for Uber to store trip information for every ride or to retain once the service is provided.

Recommendation: The Commission should require that Uber delete or anonymize this information to conform to the minimization principles of the Fair Information Practices.[55]

(6) Compel Uber to Use an Automated System to Monitor Abuses of Customer Location Data

The FTC's privacy program should prevent further abuses of customer location data by Uber employees. Abuses of "God View"—the tool that allows Uber employees to view an

[55] *See* Fair Information Practices.

individual user's real-time and historic geolocation data—was one of the most alarming privacy abuses 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."[56] Uber claimed that access to rider and driver information would be closely monitored and that violations of the policy would result in disciplinary action.[57] 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.[58] 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 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

[56] FTC Complaint at 2.
[57] *Id.*
[58] *Id.* at 3

Uber employees were monitored unless an employee was reported by a coworker.[59] 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.

Recommendation: The FTC should require Uber, as part of its mandated privacy program, to implement an automated system that closely monitors employee access to customer location data for instances of inappropriate use and require that the system be adequately monitored and reviewed.

(7) Impose Specific Requirements In The Comprehensive Privacy Program To Ensure That Third Party Data Storage Services Provide Effective Data Security

EPIC supports the requirement that Uber develop a comprehensive privacy plan to ensure that its third party service has appropriate measures in place to protect personal information. EPIC recommends that the Bureau go a step further and mandate that Uber's comprehensive privacy program include specific security measures for any third party storage service that has access to Uber's trove of personal information.

The FTC complaint detailed how Uber used Amazon Simple Storage Service (or "Amazon S3 Datastore") to store personal data.[60] The FTC stated that Uber failed to implement reasonable access controls to safeguard the data stored in the Amazon S3 Datastore by "failing to require programs and engineers that access the Amazon S3 Datastore to use distinct access

[59] *Id.*
[60] FTC Complaint at 4.

keys," and "failing to require multi-factor authentication for access to the Amazon S3 Datastore."[61]

On May 12, 2014, this storage service was the result of 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.[62] 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.[63]

Despite these allegations in the FTC's complaint, the proposed Order contains no specific provisions for how Uber will safeguard the data contained in the Amazon S3 Datastore. At a minimum, the FTC should require that any third party storage service employed by Uber implement measures that will prevent any individual from gaining full access to the entire database with one single access key.

Recommendation: The Commission should prohibit Uber from allowing a third-party storage service to permit full access to all personal data with a single, shared access key, and require any third-party storage service to implement multiple levels of encryption and anonymization of personal information within its storage system.

---

[61] FTC Complaint at 4.
[62] 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.
[63] 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/.

(8) The FTC Should Require That Uber's Privacy Assessments Are 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.[64] However, the proposed Order does not require that these privacy audits be made available to the public. As the FTC stated in its complaint, Uber collects extensive amounts of sensitive personal information from consumers. The FTC also detailed how Uber repeatedly issued false and misleading statements regarding how it monitored and secured such personal information.

In recent months, Uber has undergone a substantial loss of goodwill from the public. Uber has had to address several controversies regarding hostile work environments, harassment, and misconduct from senior executives, including its founder.[65]

In addition to a public perception problem, Uber has a history of taking steps to evade regulators and law enforcement. In March, it was widely reported that Uber had taken steps to avoid law enforcement through its "Greyball" tool.[66] 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 that existence of Greyball did so anonymously for fear of

[64] FTC Order at 3-4.
[65] Tracey Lien and David Pierson, *Uber's Self-Inflicted Controversies Come At A Price: Public Loyalty,* Los Angeles Times, Mar. 1, 2017 http://www.latimes.com/business/la-fi-tn-uber-brand-perception-20170301-story.html.
[66] 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.

being retaliated against by Uber.[67] The use of Greyabll is currently the subject of a federal inquiry by the Department of Justice.[68] 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. Despite these demands, Uber continued their self-driving car program.[69]

Releasing the mandated privacy assessments to the public is necessary to allow the public to determine whether they can safely and securely continue to use Uber's services. The FTC has acknowledged that Uber has deceived the public before and in recent months the public has repeatedly been given reasons to doubt whether Uber is capable of being fully honest with consumers. Additionally, Uber has a history of taking steps to avoid and defy regulators and law enforcement agencies in the past. The biennial privacy assessments are a good step to ensure that Uber truly does reform its privacy practices. However, to restore public trust in Uber and its services, the FTC should require the privacy audits be made available to the public.

Recommendation: The FTC should amend their proposed Order to require that Uber's Privacy Assessments are made available to the public.

---

[67] 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.
[68] 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.
[69] 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.

Conclusion

EPIC supports the Order set out by the FTC regarding Uber's past practices of issuing false and misleading statements on its privacy and security practices. But there is much more that needs to be done to address the consumer privacy concerns arising from Uber's business practices. These comments detail how the proposed Order with Uber can be strengthened to address the ongoing concerns of American consumers. Specifically, EPIC urges the Commission to allow customers to access information Uber has collected about them, prohibit the future tracking of customers, delete all improperly obtained data, impose data retention limits, impose specific requirements for privacy assessments, and to make 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. Most importantly, it is the responsibility of the FTC to protect consumer privacy and to prosecute companies that engage in unfair and deceptive trade practices.

Respectfully submitted,

/s/ Marc Rotenberg
Marc Rotenberg
EPIC President and Executive Director

/s/ Sam Lester
Sam Lester
EPIC Consumer Privacy Fellow

/s/ Kim Miller
Kim Miller
EPIC Policy Fellow

/s/ Christine Bannan
Christine Bannan
EPIC Policy Fellow