UNITED STATES OF AMERICA
Federal Trade Commission
WASHINGTON, D.C. 20580

Office of the Secretary

October 26, 2018

Marc Rotenberg, President and Executive Director
Sam Lester, Consumer Privacy Counsel
Christine Bannan, Policy Counsel
Electronic Privacy Information Center
1718 Connecticut Avenue, NW
Suite 200
Washington, D.C. 20009

Re: In the Matter of Uber Technologies, Inc., File No. 1523054

Dear Mr. Rotenberg, Mr. Lester, and Ms. Bannan:

Thank you for your comment regarding the revised proposed consent agreement that the Federal Trade Commission ("Commission" or "FTC") released for public comment in the above-entitled matter in April 2018. As you know, the revised proposed consent agreement superseded the now withdrawn proposed consent agreement that the Commission released for public comment in this matter in August 2017. The Commission greatly appreciates your feedback on the revised proposed consent agreement.

The Commission's two-count Complaint in this matter alleges that Uber Technologies, Inc. ("Uber") violated Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, by making material misrepresentations about its privacy and data security practices for personal information it collected from consumers. Count one alleges that Uber misrepresented the extent to which it monitored and audited internal access to consumers' personal information. Count two alleges that Uber misrepresented that it provided reasonable security for consumers' personal information stored in its databases. According to the Complaint, Uber's failure to reasonably secure personal information that it stored on third-party cloud servers resulted in data breaches in 2014 and 2016. The Complaint further alleges that Uber failed to disclose the 2016 data breach to the Commission until November 2017, despite the pendency of a nonpublic Commission investigation of Uber's privacy and data security practices when that breach occurred.

The proposed twenty-year Order contains provisions designed to prevent Uber from committing future violations similar to those alleged in the Complaint. The proposed Order prohibits Uber from misrepresenting the extent to which it monitors or audits internal access to, or protects the privacy, confidentiality, security, or integrity of, consumers' personal information. It requires Uber to implement and maintain a comprehensive privacy program, and to undergo, and submit to the Commission, an initial and biennial third-party assessments of the comprehensive privacy program. The proposed Order specifies that Uber's privacy program

must include consideration of foreseeable risks in each area of relevant operation, including employee training and management; product design, development, and research; secure software design, development, and testing, including access key and secret key management and secure cloud storage; review, assessment, and response to third-party vulnerability reports, including through a "bug bounty" or similar program; and prevention, detection, and response to attacks, intrusions, or system failures. The proposed Order further requires Uber to submit a report to the Commission if Uber discovers any "covered incident" involving unauthorized access or acquisition of personal information. The proposed Order also includes recordkeeping and service provisions and requirements for Uber to submit compliance reports to the Commission.

Your comment recommends that the Commission add numerous additional provisions to the proposed Order. Specifically, you recommend that the Commission require Uber to (1) provide consumers access to personal data that Uber maintains about them, (2) limit its retention of consumers' trip information after consumers complete trips, (3) implement and monitor an automated system to report inappropriate employee access to consumer data, (4) disgorge all personal data that Uber obtained unlawfully, (5) implement specific requirements to secure personal information that Uber stores in third-party data storage services, such as preventing a single access key from providing full access to the data and employing multiple levels of encryption and anonymization to ensure that sensitive information is not stored in plain-text files, and (6) maintain a bug bounty program that awards bug bounties through a clearly defined policy and without negotiation. You also recommend that the Commission prohibit Uber from (1) accessing consumers' contacts or tracking consumers when they are not using Uber's services and (2) tracking consumers' proximate locations by using their mobile phones' IP addresses.

The proposed Order is designed to address the Complaint's allegations that Uber made deceptive statements about its practices for securing and protecting the privacy of data it collected from consumers, not to impose specific obligations that may not be tied to such conduct. That said, the Commission believes that the proposed Order addresses many of the issues that your comment discusses. The comprehensive privacy program mandated by the proposed Order will require Uber to address privacy risks related to the development and management of new and existing products and services for consumers and to protect the privacy and confidentiality of consumers' personal information. Uber could face substantial civil penalties if it fails to use reasonable procedures to address foreseeable risks that could result in its unauthorized collection, use, or disclosure of consumers' personal information. The proposed Order states explicitly that Uber's comprehensive privacy program must consider a number of specific risks, including those related to access key and secret key management, secure cloud storage, and Uber's response to bug bounty reports.

Your comment further recommends that the FTC require that Uber's privacy assessments be made available to the public. Although the FTC does not publish the third-party assessments that many of its privacy and data security orders require, the Commission agrees that transparency regarding compliance with FTC orders can provide a public benefit. Thus, the public may seek access to compliance reports by requesting them under the Freedom of Information Act.[1] The Commission will make every effort to be transparent regarding

[1] 5 U.S.C. § 552 *et seq.*

compliance reports, consistent with the applicable laws. If a compliance report contains trade secrets or other confidential commercial or financial information, or information about consumers or other third parties, the Commission is prohibited from disclosing that information.[2] Upon receipt of a request for confidential treatment of all or part of a compliance report, the Commission will conduct a careful review to determine whether confidential treatment is warranted. If the Commission determines that a report has been frequently requested, the agency will post on the agency's website such portions as may be released to the public.

The Commission has placed your comment on the public record pursuant to rule 4.9(b)(6)(ii) of the Commission's Rules of Practice, 16 C.F.R. § 4.9(b)(6)(ii). Having considered all the facts of this case and all the comments submitted in response to the proposed Order, the Commission has now determined that the public interest would best be served by issuing the Complaint and Decision and Order in final form without further modifications. The final Decision and Order and other relevant materials are available from the Commission's website at http://www.ftc.gov. The Commission thanks you again for your comment.

By direction of the Commission, Commissioner Wilson not participating.

Donald S. Clark
Secretary

[2] 15 U.S.C. § 46(f) ("the Commission shall not have any authority to make public any trade secret or any commercial or financial information which is obtained from any person and which is privileged or confidential"); Commission Rule of Practice § 4.10, 16 C.F.R. § 4.10.

UNITED STATES OF AMERICA
Federal Trade Commission
WASHINGTON, D.C. 20580

Office of the Secretary

October 26, 2018

Ms. Pam Dixon
Executive Director
World Privacy Forum
4 Monroe Parkway
Suite K
Lake Oswego, OR 97035

Re: In the Matter of Uber Technologies, Inc., File No. 1523054

Dear Ms. Dixon:

Thank you for your comment regarding the revised proposed consent agreement that the Federal Trade Commission ("Commission" or "FTC") released for public comment in the above-entitled matter in April 2018. As you know, the revised proposed consent agreement superseded the now withdrawn proposed consent agreement that the Commission released for public comment in this matter in August 2017. The Commission greatly appreciates your feedback on the revised proposed consent agreement.

The Commission's two-count Complaint in this matter alleges that Uber Technologies, Inc. ("Uber") violated Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, by making material misrepresentations about its privacy and data security practices for personal information it collected from consumers. Count one alleges that Uber misrepresented the extent to which it monitored and audited internal access to consumers' personal information. Count two alleges that Uber misrepresented that it provided reasonable security for consumers' personal information stored in its databases. According to the Complaint, Uber's failure to reasonably secure personal information that it stored on third-party cloud servers resulted in data breaches in 2014 and 2016. The Complaint further alleges that Uber failed to disclose the 2016 data breach to the Commission until November 2017, despite the pendency of a nonpublic Commission investigation of Uber's privacy and data security practices when that breach occurred.

The proposed twenty-year Order contains provisions designed to prevent Uber from committing future violations similar to those alleged in the Complaint. The proposed Order prohibits Uber from misrepresenting the extent to which it monitors or audits internal access to, or protects the privacy, confidentiality, security, or integrity of, consumers' personal information. It requires Uber to implement and maintain a comprehensive privacy program, and to undergo, and submit to the Commission, an initial and biennial third-party assessments of the comprehensive privacy program. The proposed Order further requires Uber to submit a report to the Commission if Uber discovers any "covered incident" involving unauthorized access or

acquisition of personal information. The proposed Order also includes recordkeeping and service provisions and requirements for Uber to submit compliance reports to the Commission.

Your comment recommends changes to the proposed Order's requirement for Uber to obtain biennial, third-party assessments of its mandated comprehensive privacy program. Additionally, your comment recommends that the Commission hold a public workshop regarding privacy assessments.

First, you recommend that the Commission require Uber to obtain third-party audits, rather than third-party assessments, of its mandated comprehensive privacy program. In so doing, you assert that audits measure against predefined criteria while assessments measure against a standard set by the party undergoing the assessment. The Commission agrees that the mandated third-party assessments of Uber's privacy program should not be limited to determining whether Uber has complied with its own privacy standards. For that reason, the proposed Order requires a qualified, independent third-party professional to certify that Uber's privacy controls are operating effectively. The third-party professional must explain how Uber's privacy controls are appropriate in light of Uber's size, complexity, and activities, and the sensitivity of the personal information Uber collects from consumers, and are reasonable for addressing foreseeable internal and external risks that could result in Uber's unauthorized collection, use, or disclosure of consumers' personal information. In so doing, the third-party professional must explain how Uber has reasonably addressed privacy risks related to the operational areas at issue in the Complaint, including employee training and management; product design, development, and research; secure software design, development, and testing, including access key and secret key management and secure cloud storage; review, assessment, and response to third-party vulnerability reports, including through a "bug bounty" or similar program; and prevention, detection, and response to attacks, intrusions, or system failures. The Commission believes that such requirements are appropriate for addressing Uber's alleged practices in this case.

Second, you recommend that the Commission make Uber's biennial assessments public after redacting proprietary or sensitive information from them. Although the FTC does not publish the third-party assessments that many of its privacy and data security orders require, the Commission agrees that transparency regarding compliance with FTC orders can provide a public benefit. Thus, the public may seek access to compliance reports by requesting them under the Freedom of Information Act.[1] The Commission will make every effort to be transparent regarding compliance reports, consistent with the applicable laws. If a compliance report contains trade secrets or other confidential commercial or financial information, or information about consumers or other third parties, the Commission is prohibited from disclosing that information.[2] Upon receipt of a request for confidential treatment of all or part of a compliance report, the Commission will conduct a careful review to determine whether confidential treatment is warranted. If the Commission determines that a report has been frequently

[1] 5 U.S.C. § 552 *et seq.*

[2] 15 U.S.C. § 46(f) ("the Commission shall not have any authority to make public any trade secret or any commercial or financial information which is obtained from any person and which is privileged or confidential"); Commission Rule of Practice § 4.10, 16 C.F.R. § 4.10.

requested, the agency will post on the agency's website such portions as may be released to the public. Relatedly, the Commission notes that your comment states that "[t]he Commission does not require Uber to submit to the Commission any assessment after the first one, except upon request by a representative of the Commission." Under Part III of the proposed Order, Uber is in fact required to submit to the Commission each biennial assessment in addition to the initial assessment.

Finally, you recommend that the Commission hold a public workshop regarding privacy assessments, with a goal of developing a staff report on the standards, content, and procedures for privacy assessments. You raise important issues that are worth further consideration. As part of its ongoing series of hearings regarding competition and consumer protection in the 21st century, the Commission will host a data security hearing later this fall. That hearing will include discussion regarding the effectiveness of the assessment provisions in the Commission's data security orders, which are similar to the assessment provisions in the Commission's privacy orders. In addition, members of the public can submit comments related to the data security hearing or any of the other hearings in the series.

The Commission has placed your comment on the public record pursuant to rule 4.9(b)(6)(ii) of the Commission's Rules of Practice, 16 C.F.R. § 4.9(b)(6)(ii). Having considered all the facts of this case and all the comments submitted in response to the proposed Order, the Commission has now determined that the public interest would best be served by issuing the Complaint and Decision and Order in final form without further modifications. The final Decision and Order and other relevant materials are available from the Commission's website at http://www.ftc.gov. The Commission thanks you again for your comment.

By direction of the Commission, Commissioner Wilson not participating.

Donald S. Clark
Secretary

UNITED STATES OF AMERICA
Federal Trade Commission
WASHINGTON, D.C. 20580

Office of the Secretary

October 26, 2018

Mr. Robert Gellman
Washington, D.C.

Re: In the Matter of Uber Technologies, Inc., File No. 1523054

Dear Mr. Gellman:

Thank you for your comment regarding the revised proposed consent agreement that the Federal Trade Commission ("Commission" or "FTC") released for public comment in the above-entitled matter in April 2018. The revised proposed consent agreement superseded the now withdrawn proposed consent agreement that the Commission had released for public comment in this matter in August 2017. The Commission greatly appreciates your feedback on the revised proposed consent agreement.

The Commission's two-count Complaint in this matter alleges that Uber Technologies, Inc. ("Uber") violated Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, by making material misrepresentations about its privacy and data security practices for personal information it collected from consumers. Count one alleges that Uber misrepresented the extent to which it monitored and audited internal access to consumers' personal information. Count two alleges that Uber misrepresented that it provided reasonable security for consumers' personal information stored in its databases. According to the Complaint, Uber's failure to reasonably secure personal information that it stored on third-party cloud servers resulted in data breaches in 2014 and 2016. The Complaint further alleges that Uber failed to disclose the 2016 data breach to the Commission until November 2017, despite the pendency of a nonpublic Commission investigation of Uber's privacy and data security practices when that breach occurred.

The proposed twenty-year Order contains provisions designed to prevent Uber from committing future violations similar to those alleged in the Complaint. The proposed Order prohibits Uber from misrepresenting the extent to which it monitors or audits internal access to, or protects the privacy, confidentiality, security, or integrity of, consumers' personal information. It requires Uber to implement and maintain a comprehensive privacy program, and to undergo, and submit to the Commission, an initial and biennial third-party assessments of the comprehensive privacy program. The proposed Order further requires Uber to submit a report to the Commission if Uber discovers any "covered incident" involving unauthorized access or acquisition of personal information. The proposed Order also includes recordkeeping and service provisions and requirements for Uber to submit compliance reports to the Commission.

You object to the proposed Order on the grounds that it requires Uber to obtain privacy assessments rather than privacy audits "against objective standards using a thorough methodology." The Commission agrees that the mandated third-party assessments of Uber's privacy program should be objective and thorough. For that reason, the proposed Order requires a qualified, independent third-party professional to certify that Uber's privacy controls are operating effectively. The third-party professional must explain how Uber's privacy controls are appropriate in light of Uber's size, complexity, and activities, and the sensitivity of the personal information Uber collects from consumers, and are reasonable for addressing foreseeable internal and external risks that could result in Uber's unauthorized collection, use, or disclosure of consumers' personal information. In so doing, the third-party professional must explain how Uber has reasonably addressed privacy risks related to the operational areas at issue in the Complaint, including employee training and management; product design, development, and research; secure software design, development, and testing, including access key and secret key management and secure cloud storage; review, assessment, and response to third-party vulnerability reports, including through a "bug bounty" or similar program; and prevention, detection, and response to attacks, intrusions, or system failures. The Commission believes that such requirements are appropriate for addressing Uber's alleged practices in this case.

Your comment also recommends that the Commission make Uber's biennial assessments public after redacting proprietary or sensitive information from them. Although the FTC does not publish the third-party assessments that many of its privacy and data security orders require, the Commission agrees that transparency regarding compliance with FTC orders can provide a public benefit. Thus, the public may seek access to compliance reports by requesting them under the Freedom of Information Act.[1] The Commission will make every effort to be transparent regarding compliance reports, consistent with the applicable laws. If a compliance report contains trade secrets or other confidential commercial or financial information, or information about consumers or other third parties, the Commission is prohibited from disclosing that information.[2] Upon receipt of a request for confidential treatment of all or part of a compliance report, the Commission will conduct a careful review to determine whether confidential treatment is warranted. If the Commission determines that a report has been frequently requested, the agency will post on the agency's website such portions as may be released to the public.

The Commission has placed your comment on the public record pursuant to rule 4.9(b)(6)(ii) of the Commission's Rules of Practice, 16 C.F.R. § 4.9(b)(6)(ii). Having considered all the facts of this case and all the comments submitted in response to the proposed Order, the Commission has now determined that the public interest would best be served by issuing the

[1] 5 U.S.C. § 552 *et seq.*

[2] 15 U.S.C. § 46(f) ("the Commission shall not have any authority to make public any trade secret or any commercial or financial information which is obtained from any person and which is privileged or confidential"); Commission Rule of Practice § 4.10, 16 C.F.R. § 4.10.

Complaint and Decision and Order in final form without further modifications. The final Decision and Order and other relevant materials are available from the Commission's website at http://www.ftc.gov. The Commission thanks you again for your comment.

By direction of the Commission, Commissioner Wilson not participating.

Donald S. Clark
Secretary