4 Monroe Parkway
Suite K
Lake Oswego, OR 97035

Comments to the Federal Trade Commission regarding revised proposed consent decree, *In the Matter of Uber Technologies Inc*., File No. 152-3054

Via ftcpublic.commentworks.com

Federal Trade Commission
Office of the Secretary
600 Pennsylvania Avenue NW
Suite CC– 5610 (Annex D)
Washington, DC 20580

May 9, 2018

Thank you for the opportunity to comment on the revised proposed consent decree, *In the Matter of Uber Technologies, Inc.*, File No. 152–3054. The revised consent decree is at https://www.ftc.gov/system/files/documents/cases/1523054_uber_technologies_revised_complaint_0.pdf. The initial proposed consent decree appeared at https://www.ftc.gov/system/files/documents/cases/1523054_uber_technologies_decision_and_order.pdf. Relevant Federal Register citations are 82 Federal Register 39582 (August 21, 2017),[1] and 83 Federal Register 18061 (April 25, 2018).[2]

The World Privacy Forum is a non-profit public interest research group that focuses on data privacy issues, including those relating to technology, health, biometrics, and other topics. Our research, testimony, consumer education, and other materials can be found on our webpage.[3]

Our comments on the revised proposed consent decree are below.

I. Requirement for assessment

In our comments on the original 2017 proposed Uber consent decree, we requested improvements to the language regarding the requirement in the consent decree that Uber

[1] 82 Federal Register 39582 (August 21, 2017). Available at: https://www.ftc.gov/system/files/documents/federal_register_notices/2017/08/uber_published_analysis_8-21-17.pdf.
[2] https://www.federalregister.gov/documents/2018/04/25/2018-08600/uber-technologies-inc-analysis-to-aid-public-comment.
[3] World Privacy Forum home page, https://www.worldprivacyforum.org.

undertake assessments of its privacy controls. We objected that an assessment is inadequate because it falls well short of the review that an audit would provide. In the revised consent decree, the text of the assessment provision is as follows:

> III. Privacy Assessments by a Third Party
>
> IT IS FURTHER ORDERED that, in connection with its compliance with the Provision of this Order titled Mandated Privacy Program, Respondent must obtain initial and biennial assessments ("Assessments"):
> A. The Assessments must be completed by a qualified, objective, independent third-party professional, who uses procedures and standards generally accepted in the profession. An individual qualified to prepare such Assessments must have a minimum of 3 years of experience in the field of privacy and data protection. All individuals selected to complete such Assessments must be approved by the Associate Director for Enforcement, Bureau of Consumer Protection, Federal Trade Commission, in his or her sole discretion.
> Any decision not to approve an individual selected to conduct such Assessments must be accompanied by a writing setting forth in detail the reasons for denying such approval.
>
> B. The reporting period for the Assessments must cover: (1) the first 180 days after the issuance date of the Order for the initial Assessment, and (2) each 2-year period thereafter for 20 years after the issuance date of the Order for the biennial Assessments.
>
> C. Each Assessment must:
> 1. set forth the specific privacy controls that Respondent has implemented and maintained during the reporting period;
> 2. explain how such privacy controls are appropriate to Respondent's size and complexity, the nature and scope of Respondent's activities, and the sensitivity of the Personal Information;
> 3. explain how the privacy controls that have been implemented meet or exceed the protections required by the Provision of this Order titled Mandated Privacy Program; and
> 4. certify that the privacy controls are operating with sufficient effectiveness to provide reasonable assurance to protect the privacy of Personal Information and that the controls have so operated throughout the reporting period.
>
> D. Each Assessment must be completed within 60 days after the end of the reporting period to which the Assessment applies. Respondent must provide each Assessment to the Commission within 10 days after the Assessment has been completed. Respondent must notify the Commission of any portions of the Assessment containing trade secrets, commercial or financial information, or information about a consumer or other third party, for which confidential

> treatment is requested pursuant to the Commission's procedures concerning public disclosure set forth in 15 U.S.C. § 46(f) and 16 C.F.R. § 4.10.

Except for the last sentence relating to marking of confidential information, the requirement for an assessment appears to be identical to the original. The change is not material.

We continue to urge the Commission to adopt an audit requirement rather than directing companies to undertake assessments because while this requirement for assessments appears impressive on the surface, it has serious shortcomings. The obligations for an assessment are less than the obligations for an audit. **Assessment** in this context is a term of art, with specific meanings, as is the term **audit**, and the two terms are not interchangeable. We note that in the press release discussing the proposed revised consent decree, the FTC discusses an audit requirement:

> ...the new provisions in the revised proposed order include requirements for Uber to submit to the Commission all the reports from the required third-party audits of Uber's privacy program rather than only the initial such report.[4]

The confusion about the difference between an assessment and an audit is commonplace. News stories often refer to assessments as audits. See, for example, Wired, *Uber Settles with FTC Again, This Time over 2014 Privacy Breach* (August 15, 2017).[5] The article states:

> The company won't have to pay a fine, or at least it won't so long as audits show that the company is making good on its promises to ensure customers' and drivers' privacy and security."

Commission staff also sometimes refers to the assessments as audits, most recently in a September 2017 NCVHS hearing.[6]

In his book, Federal Trade Commission Privacy Law and Policy, Professor Chris Jay Hoofnagle explains the difference between an assessment and an audit.

> Although many call this requirement an audit, it is not – it is an *assessment*. In the accounting world, an audit measures compliance against some predefined criteria, such as an International Organization for Standardization (ISO) standard. As assessment is a certification of compliance with a standard set by the respondent itself. [page 167].[7]

---

[4] Federal Trade Commission, Press Releases. *Uber Agrees to Expanded Settlement with FTC Related to Privacy, Security Claims; Company failed to disclose breach in fall of 2016 during FTC investigation*. April 12, 2018. https://www.ftc.gov/news-events/press-releases/2018/04/uber-agrees-expanded-settlement-ftc-related-privacy-security.

[5] *Uber Settles with FTC Again, This Time over 2014 Privacy Breach.* Wired, August 15, 2017. https://www.wired.com/story/uber-settles-with-ftc-again-this-time-over-2014-privacy-breach/.

[6] National Committee on Vital and Health Statistics, Subcommittee on Privacy, Security, and Confidentiality, FTC Testimony, Sept. 13, 2017.

[7] CHRIS JAY HOOFNAGLE, FEDERAL TRADE COMMISSION PRIVACY LAW AND POLICY, 167, Cambridge University Press, 2016.

Further, as professor Hoofnagle observes, third-party assessments conducted by other companies under similar Commission consent decrees have been "less than rigorous" (page 167). The 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. We would like to know more about how the Commission routinely follows up with consent decrees after the initial one to 3 years of the agreement.

Because of the general confusion around the terms assessment and audit, we recommend, and in fact urge the Commission to at a minimum define *assessment*, or in some way clarify that the term assessment in fact means *audit*.

In either case, we urge the commission to insist that Uber must obtain actual audits. We observe that Facebook undertook *assessments* under a consent decree with the Commission. Yet as the recent controversies concerning Facebook's privacy practices show, assessments were worthless in uncovering operational problems, lapses, and policy shortcomings. Facebook's assessors appear to have rubberstamped Facebook's practices, and nothing useful was accomplished. There was no apparent benefit to Facebook's customers from the Commission's requirement for an assessment.

We again request (as we did in our first comments) that the audits be made available to the public with suitable redactions for any proprietary or sensitive information.

We support the Commission's requirement that the assessments or better, audits, be submitted to the Commission when conducted.

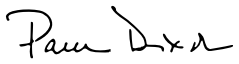
II. Request for workshop to explore/establish formal standards for privacy assessments

We request that the Commission establish formal standards for privacy assessments. It would be useful if the Commission held a public workshop on the subject of privacy assessments, with a goal of developing a staff report on the standards, content, and procedures for privacy assessments. There is also a need for clear rules governing the public disclosure of privacy assessments (or audits) mandated by the Commission.

We urge the Commission to make a meaningful attempt here so that its consent decrees have a significant effect on the privacy practices of the companies that it investigates. Mandating 20 years of assessments that do not adhere to a meaningful standard or set of known benchmarks will do little to protect the interests of consumers. Given the gravity of the Facebook/Cambridge Analytica debacle, more of the same is insufficient.

By first clearing up the confusion between assessment/audit in this proposed revision to the Uber consent decree, we believe the Commission will have made an important step forward. A staff report on the subject of privacy assessments or audits would go even further to enhance the clarity and utility of future consent decrees.

Respectfully submitted,



Pam Dixon
Executive Director
World Privacy Forum
www.worldprivacyforum.org
760-470-2000