

Review and Assessment of Uber's Privacy Program: Executive Summary

January 2015

1. EXECUTIVE SUMMARY

On November 20, 2014, Uber retained Hogan Lovells to review the Company's Privacy Program and to recommend enhancements that will further Uber's goal of being a leader in privacy and data protection. Lawyers from Hogan Lovells' Privacy and Information Management Practice assessed Uber's policies and procedures related to the handling of Consumer Data against a set of broadly accepted privacy standards, such as the expectations of the U.S. Federal Trade Commission, the Fair Information Practice Principles, and the American Institute of CPAs' Generally Accepted Privacy Principles.

Based on our in-depth review of Uber's current Privacy Program over a six-week period, we found that Uber has in place appropriate policies and procedures in each of the program elements assessed. Those elements are governance; transparency; internal access controls; third-party disclosures; privacy by design; accountability; personnel management; consumer access, inquiries, and complaints; data security; incident management and response; data retention; training and awareness; and accountability. In fact, Uber has dedicated significantly more resources to privacy than we have observed of other companies of its age, sector, and size. The Company's Privacy Program is supported by senior leadership and led by an experienced senior privacy attorney. As part of the Program, a cross-functional team including executive management meets regularly to address risks to the privacy and security of Consumer Data.

Uber's internal written privacy and security policies cover acceptable use of the Company's network, access to Consumer Data, information security, and the protection of confidential information, including Consumer Data. The Company has adopted and has implemented internal access control policies, including via technical access controls, that are reasonably designed to limit access to Consumer Data to authorized personnel. The Company regularly logs, monitors, and audits compliance with its policies.

Uber's privacy disclosures comprehensively describe the purposes for which the Company collects, uses, and discloses Consumer Data, and the Company enables consumers to review and update their personal account data. The Company has a dedicated email alias for consumers to ask privacy-related questions.

Privacy risks are considered prior to, and during, the development of new products, services, and initiatives that make use of Consumer Data. The Privacy Team reviews agreements involving the disclosure of Consumer Data to third parties, and Uber has developed standards and a centralized process for assessing and responding to law enforcement requests. Uber or its staffing agencies conduct background checks on all personnel who will have access to Consumer Data. New personnel must agree to the Company's policies pertaining to the appropriate handling of Consumer Data prior to obtaining access to that data, and Uber revokes access at the time of termination. Although its formal training program is currently in early stages of development, Uber is appropriately raising awareness of privacy protection and expectations among key stakeholders.

Uber has adopted data retention procedures for Consumer Data, including the deletion of personally identifiable information upon the cancellation of an account unless there are unresolved legal holds or account issues. While it was not in the scope of our review to perform a technical audit of Uber's data security controls, based on our review of data security policies and interviews with employees, we found that Uber has put in place and continues to develop a data security program that is reasonably designed to protect Consumer Data from unauthorized access, use, disclosure, or loss. Uber has adopted written policies and procedures that establish appropriate responsibilities and actions for reporting, investigating, mitigating, and resolving reported and identified incidents involving Consumer Data that create significant risk for the business.

Based on our review and findings, we have offered ten core recommendations for the expansion of Uber's Privacy Program. We recommend that Uber: (1) enhance its existing privacy governance framework by continuing to formalize information policies and practices, developing a concrete plan and time frame for regular reviews of the Privacy Program, and ensuring that senior leadership continues to set an appropriate tone at the top; (2) streamline and enhance the content and availability of existing privacy disclosures to help consumers more readily understand Uber's practices relating to Consumer Data; (3) implement additional tools, access controls, and written procedures that will help automate and further embed compliance with the Company's access control policies into day-to-day operations; (4) enhance its privacy by design program by further formalizing the existing privacy review of products prior to launch; (5) further formalize its vendor management program by enhancing template agreements, developing a standard set of diligence questions for vendors, and developing formal procedures to periodically review third parties' compliance with contractual and legal obligations related to data security; (6) implement additional procedures to review inactive or closed accounts that have been retained for a valid reason for a certain period of time to determine whether that reason still exists; (7) create a central "hub" for incident response resources and revise relevant policies and procedures to reflect a consistent system for classifying incident severity; (8) update the Company's written data security policies, guidelines, and templates to formally document any unwritten data security expectations for personnel related to Consumer Data; (9) enhance and formalize its training and awareness program to provide tailored trainings about Uber's privacy practices based on job responsibilities and to mandate regular refresher trainings and updated guidance; and (10) continue to emphasize employee accountability for data privacy through additional formal initiatives.

Taken together, these recommendations provide a roadmap for Uber to enhance its Privacy Program going forward in keeping with Uber's goal of being a leader in its privacy practices.