Hogan Lovells

Review and Assessment of Uber's Privacy Program

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.

2. SCOPE AND METHODOLOGY

Uber's primary business involves connecting consumers looking for rides with available drivers via the use of a mobile application (the "Uber app").[1] Uber users can request that Uber facilitate a ride via the Uber app. The Uber app locates nearby available drivers by referencing the user's location, which is set by the user or determined by the device location information ("geolocation") of the user's smartphone. After a user requests a ride, the driver who accepts the request will pick up and transport the user to the desired destination. Uber charges the user via the user's previously provided payment method. In the course of providing these services, the Company collects information about users and their rides ("Consumer Data").[2]

On November 20, 2014, Uber announced[3] that it had retained Hogan Lovells to review and assess the Company's Privacy Program, and to recommend enhancements that will further Uber's goal of being a leader in privacy and data protection. Our[4] mandate included preparing this report (the "Report"), which describes our assessment methodology, our findings, and our recommendations related to the Privacy Program.

During the course of our review, we relied upon our legal, regulatory, governance, and compliance experience to assess the Program against a set of broadly accepted privacy standards, including:

- the stated expectations of United States Federal Trade Commission ("FTC") for organizations when implementing comprehensive consumer privacy programs;[5]
- Fair Information Practice Principles ("FIPPs") for handling data relating to individuals, as expressed by various governmental organizations such as the FTC and the Organisation for Economic Co-operation and Development;[6]

---

[1] Since its launch in 2009, Uber Technologies, Inc. ("Uber" or "the Company") has experienced rapid growth. Today, the Uber app is available in over 250 cities. In the past two years, the number of Uber employees has grown from approximately 150 to over 2,000. The Company continues to expand.

[2] That information includes a user's name, contact information, payment information, device location, profile photo (if uploaded by the customer), device manufacturer and model, mobile operating system, pick-up location, destination, trip history, contact information for those with whom customers wish to share information, and information about how customers interact with the Company's interfaces (e.g., browser types, IP addresses, device identifiers, the areas of Uber's services that a user visits, and the length and frequency of visits). Our assessment of Uber's privacy compliance program for the protection of Consumer Data (the "Privacy Program") did not focus on the information that the Company collects about Uber drivers, who are independent contractors.

[3] *Strengthening Our Privacy Practices*, blog.Uber.com (Nov. 20, 2014), http://blog.uber.com/privacy-practices.

[4] Where used in this report, "we," "our," and "us" refer to Hogan Lovells.

[5] FTC, *Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers* 30 (2012), *available at* http://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf (describing controls and procedures to be included in a comprehensive privacy program that "[c]ompanies should view . . . as a roadmap as they implement privacy by design in their own organizations").

- The American Institute of CPAs' Generally Accepted Privacy Principles;[7] and
- industry-leading practices.

Drawing from these standards, we derived the following core privacy program elements to review in our assessment of Uber's Privacy Program as of the date of this report: (1) governance; (2) transparency; (3) internal access controls; (4) privacy by design; (5) consumer access, inquiries, and complaints; (6) vendor management and third-party disclosures; (7) personnel management; (8) incident management and response; (9) data retention; (10) data security; (11) training and awareness; and (12) accountability.

We developed our findings after reviewing documentation provided by Uber and interviewing senior managers and other relevant personnel from across the organization. In some instances, we were able to verify findings and have so noted in this Report. In other instances, we relied upon the presumed accuracy of the information Uber provided. We permitted Uber to review this Report in draft form to identify factual errors for our consideration.

We drew upon our findings to develop recommendations for Uber to consider as it continues to develop the Privacy Program going forward. We documented our findings and recommendations in this Report.

3. SUMMARY OF FINDINGS AND RECOMMENDATIONS

Our review found that, as of the date of this Report, Uber has a Privacy Program that includes appropriately designed and supported policies and procedures in each of the program elements assessed:

- **Governance.** Uber has put in place appropriate privacy governance. The Company has a comprehensive Privacy Program and hired an experienced Managing Counsel for Privacy in August 2014 to provide legal advice and counsel to the Company on privacy issues, including managing and directing the Privacy Program. The Program is reasonably designed to protect the privacy and confidentiality of Consumer Data and address the risks associated with the Company's collection, use, and disclosure of Consumer Data. The Managing

---

[6] Organisation for Economic Co-operation and Development, *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* 14-15 (2013), *available at* http://www.oecd.org/sti/ieconomy/2013-oecd-privacy-guidelines.pdf (Part Two – Basic Principles of National Application); FTC, *Privacy Online: A Report to Congress* 7-10 (1998), *available at* http://www.ftc.gov/sites/default/files/documents/reports/privacy-online-report-congress/priv-23a.pdf; *see also* Executive Office of the President, *Big Data: Seizing Opportunities, Preserving Values* 17-18 (2014), *available at* http://www.whitehouse.gov/sites/default/files/docs/big_data_privacy_report_may_1_2014.pdf (describing "global consensus around the FIPPs").

[7] American Institute of CPAs, *Generally Accepted Privacy Principles* (2009), *available at* http://www.aicpa.org/InterestAreas/InformationTechnology/Resources/Privacy/GenerallyAcceptedPrivacyPrinciples/Pages/default.aspx.

Counsel for Privacy continues to direct the design, implementation, and enhancement of the Privacy Program. The Company has established an appropriate tone at the top, with senior leadership emphasizing privacy in communications to employees. Uber has dedicated significantly more resources to privacy than we have observed in other companies of its age, sector, and size. The Company regularly assesses the Privacy Program and is continuing to develop controls and procedures that address privacy risks.

- **Transparency.** 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. Uber primarily describes its Consumer Data privacy practices in its online privacy policy ("Privacy Policy"). The Privacy Policy details and describes the ways in which Uber collects, uses, and discloses Consumer Data. Uber's collection and use of driver feedback on riders was disclosed in a publicly available blog post.

- **Internal Access Controls.** 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. The Company has matured from a small organization in which most employees fulfilling multiple roles required broad access to Consumer Data in order to meet business needs, to a larger organization employing a specialized workforce in which not all personnel need the same level of access. Uber has invested significant time and resources in designing, developing, and implementing an access control system tailored to the Company's workforce, network architecture, and evolving business needs.

- **Privacy by Design.** Privacy risks are considered prior to, and during, the development of new products, services, and initiatives that make use of Consumer Data. Uber has policies in place that require employees to address Consumer Data privacy issues as they arise during development of the Uber app. The Privacy Team has issued written guidance on privacy issues. Some teams have an informal practice of integrating Privacy Team review into the development of marketing and other initiatives.

- **Consumer Access, Inquiries, and Complaints.** Uber has appropriate procedures in place to allow consumers to access, update, and inquire about Consumer Data relating to them. Registered users of the Uber app can log into the Company's website or the Uber app to view their historical trips, update their profile information, and update or change their payment methods. Consumers may also obtain information about how drivers have rated them by submitting support requests.

- **Vendor Management and Third-Party Disclosures.** Uber has adopted and documented appropriate procedures to protect Consumer Data when it is shared with third parties. By written policy, the Company prohibits personnel from sharing or disclosing Consumer Data to vendors without prior approval from the Managing Counsel for Privacy. When engaging

third-party service providers that may have access to Consumer Data, Uber's policies require that any Consumer data made available to the service provider is the minimum needed to perform the service. The Company has a process in which transactions involving the disclosure of Consumer Data to a third party are reviewed by the Privacy Team. Uber has also issued a written policy establishing standards and requirements for the Company's responses to requests for Consumer Data and other information from law enforcement agencies. That policy is supported by procedures that establish a centralized process for routing and handling law enforcement requests.

- **Personnel Management.** 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 relating to the appropriate handling of Consumer Data prior to obtaining access to that data. The Company revokes personnel access to Company information systems at the time of termination.

- **Incident Management and Response.** Uber has adopted written policies and procedures that establish appropriate responsibilities and actions for reporting, investigating, mitigating, and resolving reported and identified incidents. The policies and procedures include requirements that incidents of a certain nature be documented and subject to post-mortem reporting and review.

- **Data Retention.** 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. Those issues include an account being identified as potentially fraudulent, having outstanding payments or chargebacks, and being involved in an ongoing dispute. We understand that after issues with accounts are resolved, standard cancellation procedures are followed, which include deleting personally identifiable information from Company databases containing Consumer Data.

- **Data Security.** 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. A cross-functional privacy and security team meets regularly to discuss the scope of the program, to assess potential data security risks, and to develop action items to enhance existing or implement new safeguards needed to address identified risks.

- **Training and Awareness.** 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. Employees have received communications from the CEO, the Privacy Team, and team leaders highlighting the importance of handling Consumer Data appropriately. Personnel at all levels of the organization receive at least informal training on privacy and permissible Customer Data access as a part of the

onboarding process. The Company is in the process of developing an online privacy-training module for all employees, which it plans to roll out in early 2015.

- **Accountability.** Uber communicates to personnel the standards of behavior to which the Company expects personnel to adhere through a number of methods. Those standards are described in the Company's internal policies and have been communicated to personnel by senior management, the Privacy Team, and team leaders. Through these methods, personnel are informed that violations of the Company's policies regarding the appropriate handling of Consumer Data can result in disciplinary action up to and including termination.

Our Report includes 10 recommendations to augment the Privacy Program going forward in keeping with Uber's stated goal of being an industry leader in its privacy practices. Descriptions of the recommendations are set forth in each section of the Report, and a consolidated list of all of the recommendations is attached as Appendix B. Uber has made clear its commitment to the continuous improvement of its privacy program, including by implementing enhanced monitoring and audits of personnel access to Consumer Data.

In summary, we found that Uber's Consumer Data Privacy Program is reasonably designed to address the privacy risks associated with the Company's collection, use, and sharing of Consumer Data. Specific and more detailed findings and recommendations are contained in the body of this Report.

4. REVIEW AND ASSESSMENT OF UBER PRIVACY PROGRAM

A. Introduction

This section of the Report outlines in detail, for each privacy program element assessed, the standard against which we assessed Uber's Privacy Program, our findings, and our recommendations.

B. Governance

Standard. A comprehensive, written privacy program has been implemented that is reasonably designed to address privacy risks related to the development and management of new and existing products, services, and initiatives that use Consumer Data, and to protect the privacy and confidentiality of Consumer Data. For any given company, an appropriate privacy program contains privacy controls and procedures suited to the company's size and complexity, the nature and scope of the company's activities with respect to Consumer Data, and the sensitivity of the Consumer Data held by the company. Effective governance also provides oversight, a clear allocation of responsibilities, and efficient channels for escalating and resolving actual or potential privacy control weaknesses. Key governance standards of particular relevance to Uber include:

- *Assigned responsibility and oversight*. The designation of an employee or employees to coordinate and be responsible for the privacy program.

- *Tone at the top.* The tone at the top emphasizes the importance of the appropriate protection and use of Consumer Data. Regular, ongoing, and clear communications from management promote the importance of handling Consumer Data appropriately, and the actions of senior management reflect and reinforce those communications. Tone at the top cascades from the senior executives through other layers of management and is judged by the words and actions of individual employees at all levels.

- *Adequate resources*. The provision of adequate resources and support to enable the privacy program to function.

- *Risk assessment.* The identification of reasonably foreseeable, material risks, both internal and external, that could result in the unauthorized collection, use, or disclosure of Consumer Data, and the assessment of the sufficiency of any safeguards in place to control these risks.

- *Written controls and procedures*. The design and implementation of reasonable privacy controls and procedures to address the risks identified through the privacy risk assessment, and regular testing or monitoring of the effectiveness of those privacy controls and procedures.

- *Regular evaluation and adjustment.* The adjustment of the privacy program in light of (1) the results of the regular testing and monitoring of privacy controls and procedures, (2) material changes to Uber's operations or business arrangements, and (3) any other circumstances that may have a material impact on the effectiveness of the privacy program.

Findings. We found that Uber has put in place appropriate privacy governance. The Company has a comprehensive Privacy Program and hired an experienced Managing Counsel for Privacy in August 2014 to unify and formalize the Company's approach to privacy. The Managing Counsel reports directly to the General Counsel, a member of the Leadership Team. After reviewing Program documents and interviewing relevant Uber personnel, we found that the Program is reasonably designed to protect the privacy and confidentiality of Consumer Data and address the risks associated with the Company's collection, use, and disclosure of Consumer Data. The Managing Counsel for Privacy continues to direct the design, implementation, and enhancement of the Privacy Program.

Uber's compliance with key, relevant elements of the governance standard are described below.

a. Assigned responsibility and oversight

Strong evidence of Uber's commitment to develop an industry-leading privacy program is its hiring in August 2014 of an experienced privacy attorney to fill the position of Managing Counsel for Privacy, whose primary responsibility is to provide legal advice and counsel to the Company

on privacy issues, including managing and directing the Privacy Program. The Managing Counsel reports directly to a member of the Leadership Team, which provides for the rapid escalation of issues and demonstrates the emphasis that Company leadership places on privacy.

In addition, Uber has convened a cross-functional privacy and security team charged with identifying and addressing risks that may impact the privacy and security of Consumer Data. That team is comprised of the Managing Counsel for Privacy, the Chief Technology Officer ("CTO"), the Director of Infrastructure Engineering, two senior engineering managers, an infrastructure engineer, and a senior program manager. The Managing Counsel for Privacy participates on the Team to provide legal counsel and advice when asked. Separately, employees may have privacy questions that require technical advice, which the CTO is available to address, or legal advice, which the Managing Counsel can address. The Company fosters open communications channels for privacy questions.

b. Tone at the top

Immediately after the Managing Counsel's arrival at Uber, she was asked to conduct an assessment of risks related to privacy and security of Consumer Data and to develop a roadmap for addressing the highest-priority risks. In September 2014, senior leadership directed the Managing Counsel to ensure that the Company embarks on a continuous improvement program for its privacy practices. Members of the Leadership Team and the CTO have been and continue to be directly involved in the process. In addition to her regular work with the CTO, the Managing Counsel for Privacy continues to meet with members of the Leadership Team at least once per month to provide updates on the evolution of the Privacy Program and to obtain their direct feedback on the process. Senior leadership has been directly involved in the approval of policies to formally document and enhance existing practices designed to protect Consumer Data, including requesting and establishing the timeline for the adoption of Uber's current policy on access to and use of Consumer Data.

Uber executives, including senior leadership, have backed up this commitment by emphasizing privacy in communications to employees. For example, senior leadership held an hour-long, Company-wide meeting that focused on the importance of respecting the privacy and confidentiality of Consumer Data. Moreover, during our interviews with employees, we found that they appear to have received clear communications from management that Consumer Data privacy and security are essential to maintaining consumer trust, and we have noted a general and universal appreciation of the importance of respecting the privacy and confidentiality of Consumer Data and complying with relevant policies and legal requirements. The Head of Internal Audit is developing plans to evaluate tone at the top in the context of regular audits.

c. Adequate resources

Uber has provided ample resources to the Managing Counsel for Privacy, including hiring two additional full-time, experienced privacy attorneys and a Privacy Program Manager for the core Privacy Team and providing the Privacy Team with access to supporting resources located

across Uber. In creating this four-member team tasked solely with responsibility for developing, managing, and facilitating the implementation of the Company's Privacy Program, Uber has dedicated significantly more resources to privacy than we have observed of other companies of its age, sector, and size. The Company intends to expand the Privacy Team in early 2015.

In addition to the Privacy Team, Uber has hired a Head of Internal Audit, who shares responsibility with the Managing Counsel for Privacy for auditing access to Consumer Data.

Uber continues its practice, which was in effect prior to the hiring of the Managing Counsel for Privacy, of obtaining external specialized input for significant aspects of Uber's Privacy Program, including the handling of Consumer Data. The continuing nature of this practice is evidenced by the engagement of Hogan Lovells to provide this Report.

d. Risk assessment.

The Privacy Team actively monitors legal news and updates for risks potentially affecting Consumer Data. The cross-functional privacy and security team referenced above, which includes executive management, meets regularly to address risks to the privacy and security of Consumer Data. Uber also has inventoried and classified the types of Consumer Data the Company maintains, which facilitates the assessment of risks and the identification of protections that should apply to each class of data. In sum, it is evident that privacy risk assessment is an important and ongoing process at Uber that is engrained into the Privacy Program.

e. Written controls and procedures.

In terms of documentation, the Company's Privacy Program includes written policies that establish standards for the proper handling of Consumer Data in a number of areas, including but not limited to:

- Access to and use of Consumer Data;
- Acceptable use of Company information resources;
- Information security;
- Data retention;
- Employee ethics and accountability; and
- Incident response.

Those polices are supported by administrative procedures as well as guidelines and documentation for personnel that address the Company's expectations regarding the handling of Consumer Data.

The Company continues to develop controls and procedures that address risks identified during the risk assessments described above, and are spearheading a project to roll out new privacy-related controls and procedures over the next year. This includes the development of new written policies, many of which formalize prior and existing information policies and practices.

f. Regular evaluation and adjustment.

The cross-functional team, the Privacy Team, and other stakeholders meet regularly and continually assess and improve the Privacy Program. Once the new controls and procedures have been in place for a while, the Company has indicated its intention to establish a plan and time frame for a formal evaluation and assessment of the program. At this stage of the Program's development, this is an appropriate posture to take with respect to future evaluation and assessment.

Recommendation. We recommend that Uber 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. Specific examples of how the Company can act on this recommendation include:

- Continuing to work on the task of formalizing existing information policies and practices in written form.
- Developing a concrete plan and time frame for regular reviews of the Privacy Program to determine whether the controls and procedures are operating effectively and whether there have been any material changes that would warrant updating the Program.
- Continuing to set a strong tone at the top by, for example, incorporating senior executive participation into the training of personnel on privacy policies and procedures and having senior leadership highlight how privacy considerations figure into the design or implementation of the Company's offerings.

C. Transparency

Standard. Privacy policies and other public-facing statements have been published that accurately, clearly, and conspicuously inform consumers of:

- the types of Consumer Data collected;
- the purposes for which Consumer Data is used;
- the extent to which Consumer Data is made available to third parties; and
- the extent to which consumers can control the use of data relating to them and the steps consumers can take to do so.

Findings. After reviewing Uber's privacy disclosures and interviewing relevant Uber personnel, we found that 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.

Uber primarily describes its Consumer Data practices in its Privacy Policy.[8] The Privacy Policy describes the ways in which Uber collects, uses, and discloses Consumer Data.

The Privacy Policy comprehensively describes the types of Consumer Data that Uber collects in a section titled "What Information Do We Collect?" That section is broken down into six sub-categories: "Information You Provide To Us"; "Information We Collect As You Access And Use Our Services; "Information Third Parties Provide About You"; "Information You Provide About A Third Party"; "Information Collected by Mobile Applications"; and "Information Collected from Job Applicants."[9] In our experience, this section of the Privacy Policy is more descriptive and informative than other business' privacy policies.

However, we do note that the Privacy Policy does not specifically disclose that drivers rate their experiences with riders at the end of every trip. Uber uses the feedback that drivers provide about riders ("rider ratings") to help "create and maintain a safe and respectful environment."[10] Uber has publicly disclosed the collection and use of rider ratings in a blog post in which the Company also noted that users can ask drivers or Uber support to view their ratings.

Uber thoroughly describes how it uses Consumer Data. Throughout the Privacy Policy, Uber describes how it uses the Consumer Data it collects, including to enable the Company to provide services to consumers, to facilitate compliance with the Privacy Policy itself, and to help prevent, detect and investigate fraud and non-compliance with the Company's policies.[11]

In reviewing the disclosed uses, we requested and received from the Company confirmation of the intended meaning and scope of many of the disclosed uses as well as illustrative examples.

---

[8] *Uber Privacy Policy*, Uber.com (July 13, 2013), https://www.uber.com/legal/usa/privacy. Uber has also disclosed its privacy practices in a recent blog post regarding the Company's privacy policy, in an online Android App Permissions disclosure, in a blog post addressing rider and driver ratings, and in a letter to U.S. Senator Al Franken. *Uber's Data Privacy Policy*, blog.Uber.com (Nov. 18, 2014), http://blog.uber.com/privacypolicy; *Android App Permissions*, Uber.com, https://www.uber.com/android/permissions (describing the reasons for which the Uber app requests permissions for Android devices) (last visited Jan. 22, 2015); *Feedback Is a Two-Way Street*, blog.Uber.com (Apr. 23, 2014), http://blog.uber.com/feedback; Letter from Katherine M. Tassi, Managing Counsel – Privacy, Uber, to Sen. Al Franken (Dec. 15, 2014), *available at* http://www.franken.senate.gov/files/documents/141215UberResponse.pdf.

[9] As noted previously, the information includes a user's name, contact information, payment information, device location, profile photo (if uploaded by the customer), device manufacturer and model, mobile operating system, pick-up location, destination, trip history, contact information for those with whom customers wish to share information, and information about how customer's interact with the Company's interfaces (e.g., browser types, IP addresses, device identifiers, the areas of Uber's services that a user visits, and the length and frequency of visits).

[10] *Feedback Is a Two-Way Street*, blog.Uber.com (Apr. 23, 2014), http://blog.uber.com/feedback.

[11] The data uses Uber discloses via its online privacy policy are listed in Appendix A.

For example, we requested examples of how Consumer Data is used to support internal business processes. In our experience, this is a common data use. But the interpretation of the disclosed practice can vary depending on industry sector and business. Uber informed us that the Privacy Policy enumerates the range of uses of Consumer Data and purposes that might necessitate accessing Consumer Data and that employee access and use for any of these purposes is, by definition, a legitimate business purpose. After reviewing documentation and interviewing Uber personnel about data access practices, we found that the range of permitted uses of Consumer Data by Uber employees conforms with the purposes disclosed in the Privacy Policy.[12]

Of the types of Consumer Data that Uber collects, geolocation is considered one of the more sensitive. The Federal Trade Commission and others have noted that geolocation information tied to a particular individual is sensitive due to the potential for such information to reveal an individual's daily habits, profession, personal connections, political or religious beliefs, and other details.[13] Uber is transparent about its collection of geolocation data and provides a comprehensive account of how the Company uses geolocation data.[14] The policy expressly states that Uber uses standard, industry-wide measures to secure geolocation data.

Regarding the disclosure of Consumer Data to third parties, the Privacy Policy states that (1) Uber will not sell, share, rent, or trade Consumer Data except as disclosed in the Privacy Policy or at the time of collection; (2) Uber does not share information that could reasonably be used to identify a consumer with third parties for those third parties' direct marketing purposes absent consumer consent; and (3) Uber may share Consumer Data to, among other things, fulfill certain consumer requests and to comply with law.[15]

With respect to consumer controls, the Privacy Policy, in a section titled "How Do I Change My Information and What If I Cancel My Account?", describes the ways in which consumers may update the information that they provide to Uber, modify their communications preferences, and request that their accounts be cancelled. The Privacy Policy also states that if consumers have any questions about the Policy, that they can email privacy@uber.com. That email address is monitored by members of Uber's Privacy Team.

---

[12] Our understanding is reinforced by a November 18, 2014 blog post titled "Uber's Data Privacy Policy,"[12] in which the Company stated that its employees would access Consumer Data only "for a limited set of legitimate business purposes." Listed examples of these business purposes included resolving problems in support of riders and drivers, facilitating payment transactions, monitoring for fraudulent activity, and troubleshooting bugs. All of those uses are separately permitted through other provisions in Uber's privacy policy.

[13] *See, e.g.*, FTC, *Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers* 33, 34 n.8 (2012), *available at* http://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf.

[14] Uber's Privacy Policy discloses that the Company may use geolocation data for a number of purposes, listed in Appendix A.

[15] The Privacy Policy's complete listing of instances in which the Company may share Consumer Data with third parties is contained in Appendix A.

To access the Privacy Policy through Uber's website, visitors click on the "Menu" button, which is presented at the top-left of the Company's home page and other pages under the uber.com web address. After clicking the "Menu" button, visitors are presented with a drop down list that includes a link to "Legal." After clicking on the "Legal" link, visitors are presented with the User Terms and, toward the top of the page, links to the Privacy Policy and other legal disclosures.[16]

We reviewed the Uber app available on the iOS and Android platforms and found that Uber provides access to the Company's Privacy Policy both within the Uber app and via links available in app stores, allowing potential customers to review the Privacy Policy prior to download. Within the Uber iOS app, the Privacy Policy is available in the "Legal" section of the "About" menu. The Privacy Policy is also available in the App Store via a link that is available to current or prospective customers. Within the Android app, the Privacy Policy is available via a link in the "Legal" section of the "About" menu. The Privacy Policy also is available in the Play Store via a link that is available to current or prospective customers. In addition, the online Android App Permissions notice [17] provides enhanced notice about the Android-specific repositories and systems that the app can access.[18]

In sum, we find that Uber's public-facing statements transparently disclose the intended purposes for which Consumer Data will be collected, used, and disclosed.

Recommendation. We recommend that Uber streamline and enhance the content and availability of existing privacy disclosures to help consumers more readily understand Uber's practices relating to Consumer Data. Specific examples of how the Company can act on this recommendation include:

- Streamlining the Privacy Policy to help consumers more readily understand Uber's practices relating to Consumer Data;
- Updating the Privacy Policy to clearly disclose how the Company collects and uses drivers' ratings of consumers, and how consumers may access their ratings;
- Updating the Company's website so that a conspicuous, direct link to the Uber Privacy Policy is presented in the footer of each page;
- Updating the menu structure within the Uber app so that a direct link to the Uber Privacy Policy is presented in the first level of the main menu; and
- Enhancing the already robust disclosures about the Company's processing of geolocation data by setting aside a separate section of the Privacy Policy or a separate disclosure to address the Company's use of geolocation data.

---

[16] *See Legal*, Uber.com, https://www.uber.com/legal/usa/terms, (last visited Jan. 22, 2015).

[17] *Android App Permissions*, Uber.com, https://www.uber.com/android/permissions (last visited Jan. 22, 2015).

[18] The Android App Permissions notice discloses that the Uber app requests access to various data types, which are listed in Appendix A.

D. Internal Access Controls

Standard. Procedures are implemented to manage access to Consumer Data in a manner that is reasonably designed to limit access to authorized personnel. Effective internal access controls include:

- *Role-based access.* Personnel are permitted to access Consumer Data only if needed to perform the functions of their assigned roles and responsibilities for the organization.
- *Provisioning and de-provisioning procedures.* Systems and procedures are in place to provision access to Consumer Data to personnel only when needed based on assigned roles and responsibilities. Access is de-provisioned when no longer needed (such as when employment is terminated, job roles change, or a temporary project requiring access is completed).
- *Least access.* Where possible, personnel have access to only the elements of Consumer Data necessary to perform the functions of their assigned roles and responsibilities. Access is limited to the period of time required to perform those functions. Non-necessary Consumer Data elements are, where reasonably possible, shielded through custom interfaces, anonymization, pseudonymization, or aggregation.
- *Monitoring and review of access*. Access should be monitored to determine whether personnel with access are utilizing that access in a way that complies with company access policies. Access rights should be periodically reviewed to determine whether personnel with access to Consumer Data still have a business need for that access.

Findings. Uber maintains repositories and associated interfaces that its workforce use to access Consumer Data for the purposes detailed in the Privacy Policy, including providing customer service, developing new products, and conducting marketing. After reviewing documentation and interviewing relevant personnel, we found that Uber 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.

It is apparent that Uber takes the issue of internal access to Consumer Data seriously. In the past two years, Uber's workforce has grown by over 1300%. It has matured from an organization in which most employees, while fulfilling multiple roles in the Company, required access to Consumer Data, to an organization with a more specialized workforce in which not all personnel need the same level of access to Consumer Data to fulfill legitimate business needs. The Company recognizes that consumers' contact information, trip histories, and geolocation information warrant protection, and the Company has invested significant time and resources in designing an access control system that is tailored to the organization's workforce, network architecture, and evolving business needs.

In this section, we describe the internal administrative and technical controls that Uber has developed, and continues to develop, to limit personnel access to Consumer Data.

a. Role-based access

Uber has issued a written policy stating that personnel may not access Consumer Data except for legitimate business purposes and has provided guidance interpreting what is meant by legitimate business purposes. Uber also has adopted a written data classification policy that classifies information held by the Company according to the information's potential impact on consumers and the business. One of the classifications under the data classification policy includes Consumer Data, and Uber's primary method for implementing role-based access is by applying technical access controls across that data classification at the system and application levels.

The Company also has compiled a list of job categories through its human resources management system. A cross-functional team comprised of the CTO, Managing Counsel for Privacy, Engineering Program Manager, and the Head of Technology Services has worked to determine whether each job category needs access to Consumer Data for legitimate business purposes. Examples of the job categories that Uber has determined have a business need include:

- Certain customer support representatives in order to resolve consumer inquiries or complaints about certain trips, to help consumers locate lost items, and to investigate potential fraud.
- City operations team members for purposes such as supporting rider registration and communicating with riders in accordance with the Privacy Policy.
- Engineering team members for debugging, to support investigations, and to monitor system use and efficiency.
- The Legal team to facilitate Uber's compliance with legal requests and obligations.
- The Insurance team to process insurance and accident claims.

Uber has designed role-based access controls to permit only personnel that the Company has pre-approved, based on assigned job category at the system level, to retrieve data through interfaces that provide access to Consumer Data. For job categories that do not have pre-approved access, the default is that personnel cannot retrieve information through interfaces that provide access to Consumer Data repositories. One interface allows full-time employees to write SQL queries to access certain elements of Consumer Data. This interface is monitored by Internal Audit regularly in order to prevent misuse of data, as described below in the section on "Monitoring and review of access." Uber also is actively engineering a solution to exclude employee access to personally identifiable elements of Consumer Data through this interface, and the Company ultimately is working toward a solution that will restrict access to this interface by job category.

b. Provisioning and de-provisioning procedures

While the majority of Uber's role-based access is implemented by job category, the Company has developed a process to provision access to personnel who do not have access by job category but who still have a demonstrable business need for access. These personnel are required to request approval from a director-level supervisor. If approved, the supervisor will submit the access request to the Managing Counsel for Privacy or to Information Technology directly along with the written approval. Uber has communicated these procedures and a list of supervisors with authority to review access requests to personnel through policies and Company-wide emails. The Company also is in the process of developing a custom permission management tool that will streamline this approval process and allow the Company to systematically provision access to individuals when approved, rather than having to manually approve access.

In addition to this individual approval process, Uber is developing procedures that refine the provisioning process to grant access to Consumer Data at a more granular level and via alternative models, such as peer-based permissioning. Uber also is developing a permissioning system that will automatically revoke access permissions when certain conditions (such as the expiration of temporary authorization) are met. The provisioning and de-provisioning of access for new and departing personnel during personnel onboarding and offboarding is described below in the "Personnel Management" section of the Report.

c. Least access

Uber has adopted a written policy that requires personnel to use anonymized or aggregated data whenever tasks can be reasonably accomplished by using that data. We found that Uber has developed and is continuing to develop automated tools designed to anonymize or filter out Consumer Data elements that personnel have no need to view.

For example, customer support representatives addressing a support request are presented by default with only the Consumer Data that is the proximate cause of the request. And previous interfaces that allowed personnel to view certain Consumer Data on a real-time map no longer display Consumer Data by default, instead requiring authorized personnel to retrieve Consumer Data as needed through other interfaces to which they have been granted access.[19]

d. Monitoring and review of access

Uber currently logs and audits all personnel access to Consumer Data through any interface. The Company has commenced an effort, facilitated by Internal Audit, to develop and apply algorithms that identify patterns in access logs to help detect and investigate instances of anomalous access. If an investigation reveals that personnel have accessed Consumer Data for a purpose that is prohibited by Company policy—particularly, instances of access that are not

[19] An early version of this interface, internally referred to and described by the press as "God View," was retired over a year ago and replaced with an operations tool that now masks Consumer Data.

for legitimate business purposes—the Company will take disciplinary action in accordance with policy. The Head of Internal Audit is working with data scientists to refine the algorithms for the detection of anomalous access and meets with the Privacy Team on a regular basis as part of this effort.

In addition, the Company is developing an audit program, managed by Internal Audit, which will periodically (and no less frequently than quarterly) review the access rights of personnel to determine whether access to Consumer Data repositories is appropriately allocated based on business need. This includes a review of the job categories with access to Consumer Data and a review of individuals in non-pre-approved job categories who have been granted exceptions to access data for legitimate business needs.

Recommendation. We recommend that Uber implement additional tools and written procedures that will help automate and further embed compliance with the Company's access control policies into day-to-day operations. Specific examples of how the Company can act on this recommendation include:

With respect to role-based access:

- Continuing to implement logical and technical access controls that support the role-based access program for all interfaces that provide access to Consumer Data.

With respect to provisioning and de-provisioning procedures:

- Continuing to refine and develop permissioning systems so that role-based access is more systematically and seamlessly integrated with day-to-day operations.
- Continuing to develop and implement tools that more efficiently and granularly provision and de-provision access to Consumer Data.

With respect to least access:

- Continuing to develop and implement tools and custom interfaces that enable personnel to perform their roles and responsibilities while allowing them to view only a limited subset of Consumer Data. For example, personnel with responsibilities for only a certain city could be provided with default access to Consumer Data only from that city.

With respect to the monitoring and review of access:

- Creating formal written documentation for the procedures related to the regular audits of access rights and access logs.
- Continuing to refine the development of tools used to monitor access to Consumer Data, including direct queries of Consumer Data repositories.

E. Privacy by Design

Standard. Privacy risks are considered and addressed prior to and during the development and management of new and existing products, services, and initiatives that make use of Consumer Data. For Uber, key business processes of particular relevance to privacy by design include:

- *Product Development*. The development or modification of the core app, new apps, or individual app features or functionalities that access or use Consumer Data.
- *Growth*. The research and development of initiatives to increase supply, demand, and total transactions on the Uber platform involving the use or analysis of Consumer Data.
- *Marketing*. The use of Consumer Data in marketing initiatives designed to recruit new riders or further engage existing riders.

Findings. After reviewing documentation and interviewing relevant personnel, we found that privacy risks are considered prior to, and during, the development of new products, services, and initiatives that make use of Consumer Data. Uber has policies in place that require employees to address Consumer Data privacy issues as they arise during development of the Uber app.

Specifically, the Mobile Engineering Team, which is responsible for development of the Uber app, follows written procedures that require privacy to be considered during the development process. Every new feature or functionality that is coded into the Uber app requires the Mobile Engineering Team to document in writing a number of considerations related to the new code, including the potential impact on the privacy of Consumer Data. Before the new features are shipped to consumers, the documentation must be reviewed and approved by senior engineers on the Mobile Development Team, who have been trained to identify and flag and discuss potential data collection and data usage issues with the Privacy Team. Release of the code then depends upon resolution of the privacy issues. Through this process, the Privacy Team is integrated into the app development lifecycle and has the opportunity to provide input about any privacy implications of new features or functionalities before any updates are shipped to consumers.

At Uber, the Growth Team is responsible for the research and development of initiatives to increase supply, demand, and total transactions on the Uber platform. When necessary for the testing of new initiatives, this can involve the use of Consumer Data. Such testing and development is internal to the Company and is disclosed in the privacy policy. We found that there is an informal practice for Privacy Team review of Growth initiatives to provide guidance on privacy implications. In addition, members of the Privacy Team regularly meet with and provide written guidance to the Growth Team to help identify and mitigate potential privacy risks.

We found that members of Uber's Marketing Team, which sits within Growth, are cognizant of privacy issues and informally consider privacy issues in the development of marketing campaigns. Marketing leads demonstrated a commitment to using Consumer Data only for

purposes that comply with Uber's privacy policy. A member of the Privacy Team is dedicated to providing support to the Marketing Team, and the Privacy Team provides guidance to the Marketing Team to help identify and mitigate potential privacy risks, including in the area of online marketing.

Recommendation. We recommend that Uber enhance its privacy by design program by further formalizing the existing privacy review of products prior to launch.[20]

F. Consumer Access, Inquiries, and Complaints

Standard. Consumers are able to readily access data about themselves, update that data for accuracy and completeness, and submit inquiries about the use of that data.

Findings. After interviewing relevant personnel and reviewing the Uber app and website, we found that Uber has appropriate procedures in place to allow consumers to access, update, and inquire about Consumer Data relating to them.

Registered users of the Uber app can log in to the website or the Uber app to view their historical trips, update their profile information (i.e., name, country, email address, mobile phone number, and profile photo), and update or change their payment methods. Uber's privacy policy also describes how consumers can change their account information or cancel their accounts, which they can do by submitting a support request. Uber also makes drivers' rating of consumers available to consumers, but only if a consumer submits a support request asking for the rating or asks a driver.

We found that Uber is committed to responding promptly to external support requests. The Privacy Team also monitors the privacy@uber.com email address, which is disclosed in the online privacy policy. Additionally, the support team is trained to handle privacy questions to come into the support system and escalate significant privacy questions or requests to the Privacy Team.

Recommendation. We recommend that Uber enhance its consumer access, inquiry, and complaint practices by creating an automated process for account deletion and by providing consumers with easier access to their rider rating such as through a consumer's profile page.

G. Vendor Management and Third-Party Disclosures

Standard. Prior to providing a third party with access to Consumer Data, reasonable steps are taken to (1) evaluate the capability of the third party to appropriately protect the privacy of the

[20] For example, the Company could develop a formal procedure by which the Growth Team (including Marketing) and other teams within Engineering (besides Mobile Engineering) consider privacy during the development of new features or initiatives that impact the privacy of Consumer Data. Uber could leverage the Mobile Engineering Team's development lifecycle process to create a form prompting other teams to consider whether a feature or initiative under consideration will involve novel collection, use, or disclosure of Consumer Data. If so the issue would get reviewed by the Privacy Team.

Consumer Data and (2) contractually require the third party to implement and maintain appropriate privacy protections for Consumer Data.

Findings. Uber has adopted and documented appropriate procedures to protect Consumer Data when it is shared with third parties. By written policy and in its employee handbook, Uber prohibits all personnel from sharing or disclosing Consumer Data to vendors without prior approval from the Managing Counsel for Privacy. In these policies, the Company has emphasized to employees that there are significant consequences for violations of this policy, up to and including termination. Moreover, Uber has adopted a written policy prohibiting personnel from sharing, disclosing, or demonstrating internal tools that expose Consumer Data to any third party without prior approval from a director-level supervisor, even where there is a legitimate business purpose.

When engaging with a third-party service provider, Uber's policies require that any Consumer Data made available to the service provider is the minimum needed to perform the service (e.g., data will be aggregated or anonymized where possible and data types unnecessary to the service are restricted). The Company has a process in which transactions involving the disclosure of Consumer Data to a third party are reviewed by the Privacy Team.

Uber has also issued a written policy establishing standards and requirements for the Company's responses to requests for Consumer Data and other information from law enforcement agencies. That policy is supported by procedures that establish a centralized process for routing and handling law enforcement requests. By policy, designated members of the Privacy Team evaluate all law enforcement requests, including emergency requests, on a case-by-case basis to determine whether disclosure is reasonable, appropriate, and lawful. We found that Uber has developed well-designed policies and procedures in this area that are more rigorous than we have seen in other companies of similar age and size.

Recommendation. We recommend that Uber enhance vendor management and third-party disclosure practices by further formalizing its vendor management program. Specific examples of how the Company can act on this recommendation include:

- Enhancing template agreements.
- Developing a written vendor management policy with implementing procedures that formalizes current procedures regarding vendor selection and oversight.
- Developing a standard set of diligence questions to ask of vendors that will have access to Consumer Data to determine whether vendors are able to protect the privacy and security of Consumer Data.
- Developing formal procedures to periodically review third parties' compliance with contractual and legal obligations related to privacy.

H. Personnel Management

Standard. Operational risk associated with hiring is managed through appropriate background checks and procedures for onboarding and offboarding personnel.

Findings. Based on interviews with relevant personnel, we found that prior to onboarding, Uber or its staffing agencies conduct background checks on all personnel who will have access to Consumer Data. This includes criminal record checks, Social Security number verification, and past address verification. It is the policy of the Company to not hire individuals for any positions, including those that may require access to Consumer Data, if the Company determines that the individuals have histories that suggest that they would pose a risk to the safety of consumers or that they might be at risk of misusing 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 As discussed below in the section on Training and Awareness, all Uber personnel with access to Consumer Data receive appropriate training addressing the Company's policies related to the handling of Consumer Data.

Uber also revokes personnel access to Company information systems at the time of termination. In the case of involuntary terminations, Uber revokes access to Company information systems during termination meetings.

Recommendation. We have no recommendation for personnel management.

I. Incident Management and Response

Standard. Personnel are provided with clear responsibilities and guidance regarding the investigation, resolution, and documentation of reported and identified incidents and vulnerabilities impacting Consumer Data, including data breaches.

Findings. We found that 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. For example, Uber requires reports of data loss, data misuse, technical failures, or operational failures to be processed according to the incident response procedures. The policies direct personnel to take various mitigation steps based on an assigned level of severity of the incident. Two different incident response procedures, however, provide different guidelines regarding how to classify the severity of an incident.

The policies provide a number of different internal email addresses that various personnel are asked to contact if they become aware of an incident reportable under the policies. Once an incident is reported, the policies and procedures establish responsibilities for engaging various stakeholders in the Company to participate in the incident response. For example, the Managing Counsel for Privacy has responsibility for initiating and overseeing investigations of reported incidents impacting Consumer Data, and there is a designated team, including members of the Security Engineering Team, responsible for mitigating the technical impact of incidents.

The policies and procedures also require that incidents of a certain nature be documented after the incidents are resolved, and the core incident response team must conduct a post-mortem review to identify what changes the Company can make to avoid any similar issues in the future.

Recommendation. We recommend that Uber create a central "hub" for incident response resources and revise relevant policies and procedures to reflect a consistent system for classifying incident severity.

J. Data Retention

Standard. Consumer Data is retained in personally identifiable form for a defined period of time or until a defined event occurs. The retention program includes a process to delete or de-identify such information when its retention period is complete, unless there is a legitimate business need to retain the information in identifiable form longer than the retention period, at the conclusion of which the information is deleted or de-identified.

Findings. 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. For the vast majority of account cancellation requests, we understand that Uber immediately deletes all personally identifiable information from its core business logic API, which removes that information from all other Company databases containing Consumer Data. Consumers are unable to be reasonably identified from any of the remaining information.

There are two circumstances under which personally identifiable information would be retained. The first is if Uber is subject to a litigation hold or other legal requirement, after which Uber would delete the information. The second is if an account is flagged as having an unresolved issue, such as being identified as potentially fraudulent, having negative credit, having an outstanding payment card chargeback, or being involved in an ongoing dispute with Uber. In these cases, once the issue is resolved and the flag is deleted, the account goes through the standard deletion process.

Recommendation. We recommend that Uber enhance its data retention policies and practices by implementing 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. Specific examples of how the Company can act on this recommendation include:

- Periodically auditing accounts that have been deleted by a consumer but have been retained due to a flag to determine whether the issue causing the flag still merits retention of the account.
- Implementing procedures to delete accounts that have been inactive for a prolonged period of time.

K. Data Security

Standard. The Privacy Program is complemented by an effective data security program that is reasonably designed to protect Consumer Data from unauthorized access, use, disclosure, and loss. Key elements of an effective data security program include:

- *Administrative safeguards.* Actions, policies, and procedures that are reasonably designed to manage (1) the identification of data security risks; (2) the development, implementation, and maintenance of data security measures; and (3) the conduct of personnel in relation to its impact on data security issues.

- *Technical safeguards.* Technologies that control access to data and reasonably protect data from unauthorized access, use, disclosure, and loss.

- *Physical safeguards*. Physical measures reasonably designed to protect the Company's information systems, facilities, and equipment from unauthorized intrusion and natural and environmental hazards.[21]

Findings. Data security is an integral component of any privacy program, as internal privacy controls are not effective to protect against misuse of Consumer Data if the systems storing that data are not sufficiently secure to protect against unauthorized access and loss. 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.

Under this program, the cross-functional privacy and security team meets regularly to discuss the scope of the data security program, to assess potential data security risks, and to develop action items to enhance existing or implement new safeguards needed to address identified risks. Personnel who violate policies and procedures related to data security are subject to disciplinary action, up to and including termination.

We describe Uber's adoption of specific administrative, technical, and physical safeguards in more detail below.

a. Administrative safeguards

The Company has designated responsibility for management of the data security program to managers from the Engineering, Human Resources, and Privacy Teams. These managers are members of the cross-functional privacy security team that meets on a regular basis to discuss the Company's data security program.

---

[21] In assessing Uber's data security program, we reviewed its administrative, technical, and physical safeguards in light of the detailed standards set forth in the Massachusetts Standards for the Protection of Personal Information of Residents of the Commonwealth, 201 CMR § 17.00, and in FTC guidance. *E.g.*, FTC, Protecting Personal Information: A Guide for Business (2011).

When the Managing Counsel for Privacy was hired, she was asked to conduct a privacy and data security risk assessment, to develop a roadmap for enhancing the privacy and data security posture of the Company, and to form a cross-functional team that would provide guidance to the Company and the Leadership Team on privacy and data security matters. The cross-functional privacy and security team meets regularly to discuss the scope of the security program, its ongoing progress, and any material changes in the business that reasonably implicate the security of Company data.

The cross-functional privacy and security team has proposed and made progress toward implementing a number of security controls, policies, and procedures to protect the security of Company data, including Consumer Data. For example, as a result of the project the Company has developed, implemented, and trained employees on a number of written policies that impact data security, including policies that restrict access to Consumer Data for demonstrable business purposes, set forth personnel's confidentiality obligations, and define the acceptable use of the Company's information systems. One of these written policies explains Uber's high-level information security expectations for personnel, although it emphasizes the protection of payment card data collected by the Company. Through the project, Uber plans on rolling out a number of additional security safeguards in the near future, such as refined procedures for provisioning and de-provisioning access to Consumer Data as discussed above in the section on Internal Access Controls.

In concert with the Company's data privacy and security project, the Company has appointed a Head of Internal Audit to develop and implement an audit program to regularly test and assess compliance with Uber's access controls and other security safeguards. For audit processes currently underway, the Head of Internal Audit provides regular feedback to the cross-functional privacy and security team about the effectiveness of the operation of the Company's data security controls, which the team takes into consideration when deciding whether to adopt new or modify existing controls.

As described above in the Incident Management and Response section, the Company has written procedures in place for the investigation and resolution of internal and external reports related to security vulnerabilities and incidents. Incident response procedures require the involvement of the Managing Counsel for Privacy in the event of a potential security breach impacting Consumer Data. Employees are instructed and trained to report potential security incidents via designated channels, and the support team is trained to escalate externally reported security issues. Post-mortem reviews are required for incidents involving breaches of Consumer Data.

As described above in the Vendor Management and Third-Party Disclosures section, while Uber has not developed a standard set of diligence questions for assessing the ability of vendors to adequately secure Consumer Data, all agreements that contemplate the transfer of Consumer Data to third parties are reviewed by members of the Transactions Team, who have been trained to escalate data-sharing agreements to the Managing Counsel for Privacy. Through this process, the Managing Counsel for Privacy reviews all potential data-sharing relationships and

conducts due diligence on security issues before any Consumer Data is disclosed. The Managing Counsel for Privacy also has directed physical audits of certain vendors that have access to sensitive Consumer Data, to determine whether they can adequately secure the data.

In addition, the Privacy Team has issued written guidance to the Transactions Team regarding the consideration of data security in agreements with third-party service providers that may have access to Consumer Data, and they have drafted template privacy terms that reference data security.

Data security issues are explained in the policies issued to personnel during onboarding. Uber obtains acknowledgments from personnel that they have reviewed those policies. All engineers receive security awareness training. For other personnel, the importance of data security is informally addressed on a group-by-group basis, and the Company currently is developing data security orientation for all new personnel.

The Mobile Engineering Team, which is responsible for development of the Uber app, follows written procedures that require security to be considered during the development process. The Company also has issued a written policy requiring data security to be considered throughout the development of applications and systems involved in the processing of payment card data.

b. Technical safeguards

While we did not conduct a technical security assessment, after reviewing documentation and interviewing relevant personnel we found that Uber has established appropriately designed controls for:

- centrally managing the user IDs and passwords through which personnel are authenticated on the Company's systems;
- assigning and selecting passwords and other access credentials in a random manner reasonably designed to maintain the integrity of access controls, including assigning unique user IDs and not using vendor defaults;
- requiring two-factor authentication for all employees;
- storing passwords in an encrypted, reasonably secure format;
- imposing appropriate requirements for password strength and periodic rotation of passwords;
- limiting invalid log-in attempts;
- imposing appropriate encryption requirements for Consumer Data while in transit and at rest, including full disk encryption for Consumer Data stored on laptops, smartphones, tablets, PDAs, and other mobile devices, and HTTPS/TLS encryption for Consumer Data while in transit on public and corporate networks;

- persistent monitoring of networks and access logs for signs of unauthorized access to or use of Consumer Data;
- conducting regular internal and external vulnerability scans; and
- implementing and regularly patching operating systems, firewalls, and malware protection.

Additional technical safeguards are addressed in the Internal Access Controls section of this Report.

c. Physical safeguards

Uber has established a number of physical safeguards reasonably designed to protect the Company's information systems, facilities, and equipment from unauthorized intrusion and environmental hazards, including:

- requiring visiting employees, guests, vendors, and applicants to register prior to entering the Company's headquarters;
- requiring that all equipment be secured when no authorized personnel are present;
- requiring the secure disposal of Consumer Data from storage media prior to disposal or reassignment of the media;
- requiring that physical media containing Consumer Data be encrypted prior to transportation outside of business premises; and
- establishing disaster recovery systems.

Recommendations. We recommend that Uber enhance its data security program by implementing the following additional safeguards:

a. Administrative safeguards

- 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, such as clarifying in writing that risk assessments will be conducted for all Consumer Data, not just payment card data.
- Develop a standard set of diligence questions to ask of vendors and contingent personnel that will have access to Consumer Data to determine whether they are able to protect the privacy and security of Consumer Data.
- If commercial arrangements are pursued that contemplate the sharing of Consumer Data, enhance template vendor agreements to include additional specific data security controls for consideration when entering into such agreements.

- Develop formal procedures to periodically review third parties' compliance with contractual and legal obligations related to data security.

b. Technical safeguards

- As we did not conduct a technical assessment, we did not develop recommendations on technical safeguards.

c. Physical safeguards

- Establishing written physical security policies for personnel outside of headquarters (e.g., city operations teams, remote workforce members).

To the extent that recommendations contained in the Governance, Vendor Management and Third-Party Disclosures, and Incident Management and Response sections of this Report impact data security, Uber should incorporate those recommendations into its plans for the data security program as well.

L. Training and Awareness

Standard. Privacy training for all personnel with access to Consumer Data covers the Privacy Program, emphasizes the importance of compliance with privacy obligations, highlights relevant privacy risks, and provides guidance on how to mitigate privacy risks. Specifically, the privacy training gives consideration to:

- Initial training for personnel addressing the importance of appropriate handling of Consumer Data;
- Ongoing awareness activities, targeting personnel as appropriate;
- Training modules tailored for specific workforce roles;
- Refresher training for all personnel on a periodic basis; and
- Tracking of personnel training via a learning management system to document that personnel complete required training modules.

Findings. After reviewing documentation and interviewing relevant personnel, we found that 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. Employees have received communications from the CEO, the Privacy Team, and team leaders highlighting the importance of handling Consumer Data appropriately. Particularly, the Privacy Team has actively reached out to groups within the Company to make the team available as a resource and has provided guidance on privacy issues to explain the implications of the Company's role-based access controls.

Personnel at all levels of the organization receive at least informal training on privacy and permissible Customer Data access as a part of the onboarding process. Managers frequently deliver on-the-job training to employees regarding appropriate access to and use of Consumer Data. The Company is in the process of developing an online privacy-training module for all employees, which it plans to roll out in early 2015.

Recommendation. We recommend that Uber 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. Examples of how the Company can act on this recommendation include:

- Continuing to develop and roll out the online privacy-training module as planned.
- Regularly updating guidelines that clarify to personnel the legitimate business purposes for which personnel may access Consumer Data.

M. Accountability

Standard. Compliance with policies and procedures related to Consumer Data and responsible use of Consumer Data is emphasized. Key accountability standards of particular relevance for Uber include:

- Personnel should be aware of the standards of behavior to which Uber expects them to adhere, including the detailed, unambiguous expectations and requirements articulated in policy documents and communicated through training.
- Personnel should be aware of their personal accountability and responsibility for handling Consumer Data appropriately.
- Personnel should be encouraged to seek clarification and support if they are unsure what they should do in any situation involving the handling of Consumer Data.
- Personnel should be encouraged to escalate issues that they believe may result in risks to Consumer Data.
- There should be clear consequences for any personnel who violate the Company's policies and procedures related to Consumer Data. Depending on the severity of the violation, the consequences may involve disciplinary action, including counseling, probation, suspension, or dismissal.

Findings. After reviewing documentation and interviewing relevant personnel, we found that Uber communicates to personnel the standards of behavior to which the Company expects personnel to adhere through a number of methods. Those standards are described in the Company's internal policies and have been communicated to personnel by senior management, the Privacy Team, and team leaders. Communications from the Privacy Team have encouraged

personnel to contact the Privacy Team or the CTO with questions about the Company's data access policies.

Through these methods, personnel are informed that violations of the Company's policies regarding the appropriate handling of Consumer Data can result in disciplinary action up to and including termination. To supplement existing measures, the Company is developing a formal plan for Human Resources to assess the severity of data access violations and issue appropriate discipline.

Recommendation. We recommend that Uber continue to emphasize employee accountability for data privacy through additional formal initiatives, including further embedding data privacy into existing or new important Company processes. Examples of how the Company can act on this recommendation include:

- Implementing a well-publicized whistleblowing hotline to receive reports from personnel.
- Integrating personnel contributions to the promotion of consumer privacy into performance evaluations.
- Emphasizing the importance of consumer privacy in the Company's Code of Ethics.

5. APPENDICES

Appendix A: Digest of Uber's Privacy Policy

The data uses Uber discloses via its Privacy Policy include the following:

- providing services to users, including facilitating transportation connections;
- operating, enhancing, and improving the Company's services;
- processing user registrations and transactions;
- determining fees for services;
- charging users for services rendered;
- enabling users to participate in promotions, contests, or sweepstakes;
- providing users with information about how they have used the Company's services;
- facilitating software updates and product support;
- sending users communications, promotions, and offers;
- supporting internal business purposes;
- engaging in practices disclosed at the time of collection;
- learning how users interact with the Company's services and communications;
- sharing information with others as requested by users;
- generating aggregated or anonymized information for statistical analysis;
- preventing, discovering, and investigating potential violations of the privacy policy, Uber's terms of service, or the terms of use for the Uber app;
- investigating fraud, chargebacks, and other issues; and
- customizing and personalizing content, services, and communications for users.

Uber's Privacy Policy discloses that the Company may use geolocation data for the following purposes:

- enabling drivers and riders to connect;
- operating, enhancing, and improving the Company's services;

- determining charges for transportation services requested via the Uber app;
- providing customer support;
- sending promotions and offers to users;
- customizing content, services, and communications;
- supporting internal business purposes;
- creating aggregated and anonymized information to support analytics;
- preventing, discovering, and investigating potential violations of the privacy policy, Uber's terms of service, or the terms of use for the Uber app; and
- investigating fraud, chargebacks, and other issues.

Uber's Privacy Policy discloses the following instances in which the Company may share Consumer Data with third parties:

- to fulfill consumer requests to receive information or marketing offers from third parties;
- with third-party providers that perform services on behalf of Uber, limiting the information provided to that which is needed to perform the services and requiring those providers to use and disclose identifiable Consumer Data only to perform services for Uber;
- with Uber's parent, subsidiaries, or affiliates;
- with subsequent owners, co-owners, or operators of the Company's services or databases;
- in connection with a merger, consolidation, restructuring, sale of substantially of Uber's membership interests or assets, or other corporate change, including during due diligence processes;
- to provide co-branded services that Uber provides in association with third parties;
- to conduct sweepstakes, contest, and promotions that consumers choose to enter; and
- as Uber reasonably determines necessary and appropriate to:
    - comply with applicable laws, regulations, subpoenas, governmental requests, or legal process;
    - protect and defend the Company's terms of service and other applicable policies, including investigations of potential violations;

- protect the safety, rights, property, or security of Uber, its services, or third parties;
- protect the safety of the public;
- detect, prevent, or otherwise address fraud, security, or technical issues;
- prevent or stop activity that Uber considers to be, or to pose a risk of being, illegal, unethical, or legally actionable; and
- cooperate with third-party copyright owners, Internet service providers, wireless service providers, and law enforcement.

The Android App Permissions notice discloses that the Uber app requests access to the following:

- Identity to facilitate registrations for users with Google Sign-In or Google Wallet accounts, to enable Google+ account users to sign into the Uber app, and to facilitate payment transactions for users with Google Wallet accounts;
- Contacts/Calendar to support fare-sharing requests and to prepopulate certain registration fields;
- Location to personalize the user experience; display trip histories in receipts; facilitate driver selection and pickup; identify relevant products, promotions, and surveys; facilitate analytics of aggregated data; and customize and improve the Company's location-based services;
- Phone to enable users to call drivers from the Uber app;
- Photos/Media/Files to enable the Company to save map data to external storage in order to reduce the need to download map data every time the Uber app is used;
- Camera/Microphone to enable users to use the camera to scan credit cards rather than manually entering payment information;
- Wi-Fi Connection Information to help optimize the data used to display maps;
- Device ID & Call Information to prepopulate mobile phone numbers and countries during registration and to facilitate fraud prevention;
- Use Accounts on the Device to enable Uber to send notifications to users;
- Read Google Service Configuration to enable the Uber app to use web-based services, including the Google Maps API;
- Modify System Settings to optimize the data used to display maps;

- Full Network Access to allow the Uber app to access the Internet;
- Control Vibration to allow the Uber app to vibrate the phone when the Uber app issues notifications;
- Prevent Phone from Sleeping to wake a user's phone when a notification is received; and
- Use Network Connections to notify users when a network connection is not available.

Appendix B: Consolidated List of Recommendations

Taken together, the following recommendations provide a high-level roadmap for Uber to use in enhancing the Privacy Program going forward.

Governance

We recommend that Uber 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. Specific examples of how the Company can act on this recommendation include:

- Continuing to work on the task of formalizing existing information policies and practices in written form.
- Developing a concrete plan and time frame for regular reviews of the Privacy Program to determine whether the controls and procedures are operating effectively and whether there have been any material changes that would warrant updating the Program.
- Continuing to set a strong tone at the top by, for example, incorporating senior executive participation into the training of personnel on privacy policies and procedures and having senior leadership highlight how privacy considerations figure into the design or implementation of the Company's offerings.

Transparency

We recommend that Uber streamline and enhance the content and availability of existing privacy disclosures to help consumers more readily understand Uber's practices relating to Consumer Data. Specific examples of how the Company can act on this recommendation include:

- Streamlining the Privacy Policy to help consumers more readily understand Uber's practices relating to Consumer Data;
- Updating the Privacy Policy to clearly disclose how the Company collects and uses drivers' ratings of consumers, and how consumers may access their ratings;
- Updating the Company's website so that a conspicuous, direct link to the Uber Privacy Policy is presented in the footer of each page;
- Updating the menu structure within the Uber app so that a direct link to the Uber Privacy Policy is presented in the first level of the main menu; and

- Enhancing the already robust disclosures about the Company's processing of geolocation data by setting aside a separate section of the Privacy Policy or a separate disclosure to address the Company's use of geolocation data.

Internal Access Controls

We recommend that Uber implement additional tools and written procedures that will help automate and further embed compliance with the Company's access control policies into day-to-day operations. Specific examples of how the Company can act on this recommendation include:

With respect to role-based access:

- Continuing to implement logical and technical access controls that support the role-based access program for all interfaces that provide access to Consumer Data.

With respect to provisioning and de-provisioning procedures:

- Continuing to refine and develop permissioning systems so that role-based access is more systematically and seamlessly integrated with day-to-day operations.

- Continuing to develop and implement tools that more efficiently and granularly provision and de-provision access to Consumer Data.

With respect to least access:

- Continuing to develop and implement tools and custom interfaces that enable personnel to perform their roles and responsibilities while allowing them to view only a limited subset of Consumer Data. For example, personnel with responsibilities for only a certain city could be provided with default access to Consumer Data only from that city.

With respect to the monitoring and review of access:

- Creating formal written documentation for the procedures related to the regular audits of access rights and access logs.

- Continuing to refine the development of tools used to monitor access to Consumer Data, including direct queries of Consumer Data repositories.

Privacy by Design

We recommend that Uber enhance its privacy by design program by further formalizing the existing privacy review of products prior to launch.

Consumer Access, Inquiries and Requests

We recommend that Uber enhance its consumer access, inquiry, and complaint practices by creating an automated process for account deletion and by providing consumers with easier access to their rider rating such as through a consumer's profile page.

Vendor Management and Third-Party Disclosures

We recommend that Uber enhance vendor management and third-party disclosure practices by further formalizing its vendor management program. Specific examples of how the Company can act on this recommendation include:

- Enhancing template agreements.
- Developing a written vendor management policy with implementing procedures that formalizes current procedures regarding vendor selection and oversight.
- Developing a standard set of diligence questions to ask of vendors that will have access to Consumer Data to determine whether vendors are able to protect the privacy and security of Consumer Data.
- Developing formal procedures to periodically review third parties' compliance with contractual and legal obligations related to privacy.

Personnel Management

We have no recommendation for personnel management.

Incident Management and Response

We recommend that Uber create a central "hub" for incident response resources and revise relevant policies and procedures to reflect a consistent system for classifying incident severity.

Data Retention

We recommend that Uber enhance its data retention policies and practices by implementing 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. Specific examples of how the Company can act on this recommendation include:

- Periodically auditing accounts that have been deleted by a consumer but have been retained due to a flag to determine whether the issue causing the flag still merits retention of the account.
- Implementing procedures to delete accounts that have been inactive for a prolonged period of time.

Data Security[22]

We recommend that Uber enhance its data security program by implementing the following additional administrative and physical safeguards:

With respect to administrative safeguards:

- 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, such as clarifying in writing that risk assessments will be conducted for all Consumer Data, not just payment card data;
- Develop a standard set of diligence questions to ask of vendors and contingent personnel that will have access to Consumer Data to determine whether they are able to protect the privacy and security of Consumer Data;
- If commercial arrangements are pursued that contemplate the sharing of Consumer Data, enhance template vendor agreements to include additional specific data security controls for consideration when entering into such agreements;
- Develop formal procedures to periodically review third parties' compliance with contractual and legal obligations related to data security.

With respect to physical safeguards:

- Establish written physical security policies for personnel outside of headquarters (e.g., city operations teams, remote workforce members).

Training and Awareness

We recommend that Uber 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. Examples of how the Company can act on this recommendation include:

- Continuing to develop and roll out the online privacy-training module as planned.
- Regularly updating guidelines that clarify to personnel the legitimate business purposes for which personnel may access Consumer Data.

[22] To the extent that recommendations contained in the Governance, Vendor Management and Third-Party Disclosures, and Incident Management and Response sections of this Report impact data security, Uber should incorporate those recommendations into its plans for the data security program as well.

Accountability

We recommend that Uber continue to emphasize employee accountability for data privacy through additional formal initiatives, including further embedding data privacy into existing or new important Company processes. Examples of how the Company can act on this recommendation include:

- Implementing a well-publicized whistleblowing hotline to receive reports from personnel.
- Integrating personnel contributions to the promotion of consumer privacy into performance evaluations.
- Emphasizing the importance of consumer privacy in the Company's Code of Ethics.