SEPTEMBER 2017

CYBERSECURITY BULLETIN

Borden Ladner Gervais

Settlement of Uber Privacy/Data Security Complaint – Cybersecurity Guidance

On August 15, 2017, the U.S. Federal Trade Commission (FTC) *announced* that Uber agreed to settle an FTC complaint regarding Uber's alleged deceptive representations about its privacy and data security practices. The complaint and settlement provide useful cybersecurity guidance.

The Complaint

The FTC's *complaint* alleged that Uber failed to provide reasonable security for consumers' personal information stored in Uber's databases (including data stored in a commercial cloud service), contrary to Uber's privacy policy and public statements about its data security practices.

In particular, the complaint alleged that Uber's data security practices were deficient in the following respects:

- **Written Program:** Failure to have a written information security program.
- **Training:** Failure to implement reasonable security training and guidance.
- **Encryption:** Storing sensitive personal information in readable text rather than encrypting the information.
- **Access Controls**: Failure to implement reasonable access controls to safeguard stored personal information, including requiring individuals to use distinct access keys (rather than sharing an access key), restricting access based on job functions, and requiring multi-factor authentication for access to cloud data stores.
- **Monitoring:** Failure to have a system that effectively monitors access to consumer's personal information by employees and contract workers.

The complaint alleged that Uber could have prevented or mitigated the alleged data security deficiencies "through relatively low-cost measures".

The complaint also alleged that, as a result of Uber's data security deficiencies, an intruder was able to gain unauthorized access to consumers' personal information (including 100,000 unencrypted names and driver's license numbers) stored by Uber in a commercial cloud service.

The Settlement Agreement

The *settlement agreement* prohibits Uber from making any false statements regarding Uber's privacy and data security practices.

The settlement agreement requires Uber to establish, implement and maintain a comprehensive, documented privacy program that is reasonably designed to address privacy risks relating to existing and new products and services and to protect the privacy and confidentiality of personal information. The privacy program must contain controls and procedures appropriate to Uber's size and complexity, the nature and scope of Uber's activities, and the sensitivity of personal information collected or received by Uber. In particular, the privacy program must include the following:

- **Accountability:** Designated employees responsible for the privacy program.
- **Risk Assessment:** An assessment of internal and external risks in each area of Uber's operations (including employee training and management and product design, development and research) that could result in the unauthorized collection, use or disclosure of personal information, and an assessment of the sufficiency of existing safeguards to control those risks.
- **Security Measures:** The design and implementation of security controls to address identified risks, and regular testing/monitoring the effectiveness of those controls.
- **Service Providers:** The use of reasonable procedures regarding the selection of service providers capable of protecting personal information received from Uber, and contract provisions that require service providers to protect personal information.
- **Periodic Assessments/Adjustments:** The assessment and adjustment of the privacy program in light of the results of periodic testing and monitoring, changes to operations or business arrangements, and other circumstances that may impact the effectiveness of the privacy program.

The settlement agreement also requires Uber to obtain biennial, independent assessments of Uber's compliance with the agreement.

Comment

The data security measures required by the settlement agreement, and the guidance implied in the FTC complaint, are consistent with guidance issued by the FTC, including *Start with Security – A Guide for Business*, *Protecting Personal Information: A Guide for Business*, and the *Stick with Security* blog posts.

The data security measures required by the settlement agreement are also consistent with Canadian personal information protection laws, which provide that organizations are accountable for the information they collect and must protect personal information using appropriate safeguards. Following is a summary of those fundamental principles:

- **Accountability:** An organization is responsible for personal information in the organization's possession or under the organization's control, including information the organization has transferred to a third party for processing or to provide services to the organization. An organization is required to use contractual or other means to provide a comparable level of protection while personal information is being processed by a third party. An organization is required to implement policies and practices to give effect to applicable legal restrictions and requirements, including implementing internal procedures to protect personal information and training staff about the organization's policies and practices. The Canadian Privacy Commissioner's *Interpretation Bulletin: Accountability* provides a detailed discussion of the accountability principle.
- **Safeguards:** An organization must protect personal information (while in transit and while at rest) using "security safeguards appropriate to the sensitivity of the information". The required safeguards must protect personal information (regardless of the format in which the information is held) against loss or theft, as well as unauthorized access, disclosure, copying, use or modification. The nature of the required safeguards will vary depending on the sensitivity of the information, the amount, distribution and format of the information, and the method of storage. The safeguards should include physical measures, organizational measures and technological measures. An organization must make its employees aware of the importance of maintaining the confidentiality of personal information. When an organization no longer requires personal information, the organization must securely delete or destroy the personal information. The Canadian Privacy Commissioner's *Interpretation Bulletin: Safeguards* provides a detailed discussion of the safeguards principle.

Canadian privacy commissioners have issued helpful guidance for protecting personal information. For example: *Getting Accountability Right with a Privacy Management Program*; *Privacy Toolkit for Businesses – A Guide for Businesses and Organizations*; *Securing Personal Information: A Self-Assessment Tool for Organizations*; *Reaching for the Cloud(s): Privacy Issues related to Cloud Computing*; *Cloud Computing for Small- and Medium-Sized Enterprises: Privacy Responsibilities and Considerations*; *Processing Personal Data Across Borders: Guidelines*; and *Thinking About Clouds? Privacy, security and compliance considerations for Ontario public sector institutions*. ■

Author

Bradley J. Freedman
T 604.640.4129
bfreedman@blg.com

BLG's Cybersecurity Law Group assists clients with legal advice to help manage cyber risks and to respond to data security incidents. Information about BLG's Cybersecurity Law Group is available at blg.com/cybersecurity.

BLG Cybersecurity Group – Key Contacts

Bradley J. Freedman	Vancouver	604.640.4129
Éloïse Gratton	Montréal	514.954.3106
Kevin L. LaRoche	Ottawa	613.787.3516
David Madsen	Calgary	403.232.9612
Ira Nishisato	Toronto	416.367.6349

BLG Vancouver
1200 Waterfront Centre, 200 Burrard St
Vancouver, BC, Canada V7X 1T2
T 604.687.5744 | F 604.687.1415
blg.com