BUSINESSCLASS
KNOWLEDGE ▪ SEMINARS ▪ INSIGHTS

Blakes

Big Data, Big Risk?

Privacy and Security Tips for Fintech Companies

By Wendy Mee

Many fintech companies collect and process vast amounts of data in order to provide financial services quickly and inexpensively. Much of this data is highly sensitive personal information such as date of birth, social insurance number, bank account details, online banking credentials and credit score. The sheer volume of the information increases its sensitivity because over time a fintech company may generate a very detailed and complete picture of an individual. As a result, data security and compliance with applicable privacy legislation are of critical importance. Here are four privacy and security tips for fintech companies.

1 Build privacy protective controls and security safeguards into the technology as it is developed.

For a young fintech company, a data breach could have devastating impacts on customer trust and investor confidence, so most fintech companies are taking privacy and data security seriously. Fintech companies may even have an advantage over existing financial services providers in this regard, since they can build privacy protective controls and security safeguards into the technology as it is developed, rather than having to fit them into existing processes and systems retroactively.

2 Develop and operationalize robust information governance programs.

Because of the rapid pace at which fintech is developed and commercialized, fintech companies may be pushed to start collecting and processing personal information before their privacy and security frameworks are fully developed. This creates unnecessary risk from a privacy and security perspective.

During the Office of the Privacy Commissioner of Canada's (OPC) investigation into the Ashley Madison data breach, Avid Life Media Inc. (ALM), operator of the Ashley Madison website, admitted that it had gone through a rapid period of growth leading up to the time of the data breach and that it was, at that time, in the process of documenting its security procedures and improving its information security posture.

Although the OPC's report did not go so far as to conclude that this caused the data breach, it did caution that "it is not sufficient for an organization . . . that holds large amounts of personal information of a sensitive nature, to address information security without an adequate and

coherent governance framework." It also noted that while ALM was a relatively small organization (approximately 100 employees), in light of the quantity and sensitivity of the information it collected it nevertheless should have implemented a comprehensive information security program. Accordingly, fintech companies of all sizes would be well advised to develop and operationalize robust information governance programs before collecting and processing personal data.

3 Be aware of the challenges in different jurisdictions.

Fintech companies also face privacy challenges when expanding a product or service offering developed for one jurisdiction to another jurisdiction with different privacy and data protection rules. For example, when launching in Canada, many U.S. offerings need to be modified to account for Canada's broad definition of personal information.

Canadian privacy laws define personal information as information about an identifiable individual. According to case law, information will be about an identifiable individual if there is a serious possibility that the individual could be identified from the information, whether alone or in combination with other information. Accordingly, information about an individual's online or offline behaviour that is tracked to a unique identifier (such as a device ID, app ID or IP address) will generally be considered personal information in Canada, even if the individual is not actually identified by name or even if the individual is not identifiable to all users of a particular system.

Fintech companies also need to keep in mind that in Canada, even publicly available personal information is subject to Canadian privacy laws. This means that subject to limited exceptions, publicly available personal information can only be collected, used and disclosed by an organization with the consent of the data subject. This is of particular relevance for those fintech companies that collect data from public sources for analytics and automated decisioning.

4 Limit retention of personal information and understand what it means for information to be truly "anonymous."

As mentioned above, the broad definition of personal information in Canada means that information that may not be subject to regulation in other jurisdictions (such as the United States) is subject to Canadian privacy laws. This raises a number of challenges for fintech companies, including with respect to data retention. Under Canadian privacy laws, personal information can only be retained for as long as necessary to fulfil the purposes for which it was collected. Personal information that is no longer required must be destroyed, erased or anonymized.

Many fintech business models rely on the ability to generate actionable insights from vast amounts of data, and it is often not commercially practical to delete or destroy data after a service has been provided to a customer. Accordingly, many fintech companies are turning to anonymization as an alternative. However, to be truly anonymous, information must no longer be "personal information," which is a difficult standard to meet in Canada. For example, simply replacing direct identifiers such as name and address with unique codes will not result in true anonymization. Further, fintech companies will be challenged with finding a balance between effective anonymization and retaining the utility of the data.

CONTACT

For further information, please contact Wendy Mee or any other member of our Privacy or Fintech groups.

Blakes