PRIVACY IMPLICATIONS OF AN OPEN BANKING SYSTEM IN CANADA

Posted on October 12, 2021

Categories: Insights, Publications

In August, Canada's Advisory Committee on Open Banking (the "**Committee**") released its final report (the "**Final Report**"), which provides the Committee's recommendations for how Canada should implement an open banking system. Since then, as part of their platform for reelection, the liberal government promised to move forward with a "made-in-Canada" open banking system that will launch no later than the beginning of 2023. Now that a liberal government has been reinstated, we anticipate ongoing development of Canada's open banking system.

This bulletin will focus primarily on the privacy and data security implications of an open banking rollout in Canada, and what related changes financial institutions and financial tech companies ("**fintechs**") ought to consider as the government installs the new framework. Please see our August 2021 bulletin for an overview of the recommendations contained in the Final Report. You can also find general information about open banking in our previous bulletins on the topic from February and July 2019.

What is open banking?

Open banking is a regulatory framework that allows individuals and businesses to safely and securely share banking and transaction data with authorized third parties. By enabling the safe and secure access to information, open banking would allow fintechs to develop a new suite of useful financial services apps and products for the benefit of individuals and businesses. These services could range from budget-tracking, to tax assistance, to alternative credit worthiness measurements or addiction management tools.

Some fintechs already access consumers' financial data through "screen scraping", a crude process which directly copies information available on a consumer's financial account. However, screen scraping presents a significant threat to consumer privacy, since it frequently requires the consumer to disclose their banking login credentials and password. Furthermore, it may leave consumers without recourse if their information is accessed without authorization or misused.[1] An open banking framework would facilitate a shift away from screen-scraping towards a system that offers more safeguards to consumers and enhanced competition within the financial sector.

Privacy and Open Banking

Since open banking is predicated on the free flow of information, privacy is key to an open banking system. In its February 2019 Review into the Merits of Open Banking, the Committee said "[t]he trust needed to allow the digital economy to flourish, and the social license that organizations will need from Canadians to innovate with their personal data, hinges on having an appropriate legal framework in place that puts at the forefront key privacy issues." In its January 2020 review of stakeholder submissions, the Committee observed that all stakeholders considered privacy to be a significant risk of open banking.[2] In its own submission to the Committee, the Office of the Privacy Commissioner of Canada ("**OPC**") called for several privacy reforms to support an open banking system.[3]

Many of those reforms are already making progress. Before the election was called, the government had introduced a substantive overhaul to Canada's *Personal Information Protection and Electronic Documents Act* ("**PIPEDA**"), in the form of Bill C-11, which would have enacted the *Consumer Privacy Protection Act* ("**CPPA**") (we summarized the proposed changes in a previous bulletin). Bill C-11 died on the order paper when the election was called, but since the liberal government has now returned to office, a new privacy law bill is expected to be forthcoming. There is added international pressure for privacy reforms too, as the EU reviews Canada's adequacy status under the General Data Protection Regulation ("**GDPR**"). Maintaining such status is crucial as it permits data processed in accordance with the GDPR to be subsequently transferred from the EU to Canada without requiring additional data protection safeguards or authorization to transfer the data.

Meanwhile in Quebec, *An Act to modernize legislative provisions as regards the protection of personal information* ("**Bill 64**") received Royal Assent on September 22, 2021. This Bill amends Quebec's *Act respecting the protection of personal information in the private sector* ("**Quebec's Private Sector Act**") to include a data portability right, increased fines for non-compliance, and enhanced requirements for breach notification, consent, and data protection, among other changes.

So what further developments might we see on the horizon as the Canadian government implements an open banking system? And how should prospective open banking participants respond?

Data Portability

In its June 2019 report on open banking, the Standing Senate Committee on Banking, Trade and Commerce recommended modernizing PIPEDA to align it with global privacy standards. It wrote that these changes "must include a consumer data portability right."

In the context of open banking, data portability means a consumer's right to direct that their personal financial information be shared with another organization. While this sounds simple in theory, it presents challenges for

the organization sharing the data (typically the financial institution). First, personal information owned by the consumer is often grouped together with information owned by the sharing organization. For example, financial institutions may create "derived data" by processing consumer information together with proprietary algorithms and analysis.[4] The Final Report takes the position that the financial institution should generally be able to exclude derived data from an open banking system. However, if such data is normally available to the consumer, the financial institution should have an obligation to justify an exclusion.[5]

The second and related challenge is that sharing organizations may store and process data in a variety of formats, but for data portability to be meaningful, the personal information must be shared in a usable technological form. The difference between a string of loose data, and a properly organized spreadsheet is significant to the utility of such information for a third party app developer. Financial institutions can look to Quebec's Bill 64 as an example of how the concept of data portability could play out in practice. When it comes into force, Bill 64 will amend Quebec's Private Sector Act to provide consumers with a right to request their computerized personal information in a "structured, commonly used technological format" unless doing so raises serious practical difficulties.[6]

The introduction of a data portability right may require financial institutions to overhaul their data processing systems to ensure consumer data can be shared in a commonly used form, while separating out data that is unnecessary or proprietary to the financial institution. Depending on the sharing organization's data processing systems, data portability may require significant lead time to implement. The challenges outlined above are likely why the technological format amendment to Quebec's Private Sector Act does not come into force until September 22, 2024 (a full year after the majority of the amendments).

Data Security

From a technical standpoint, open banking requires financial institutions to make their application programming interface ("**API**") freely available to accredited, authorized third parties. This increased level of connectivity naturally comes with increased risk of fraud, financial crime and/or data breaches.

Furthermore, PIPEDA requires organizations to implement security safeguards commensurate to the sensitivity of the information,[7] and financial information has been recognized as "extremely sensitive" by the OPC and the Supreme Court of Canada.[8] Accordingly, open banking participants should expect strict data protection requirements to be introduced as part of an open banking framework.

The Final Report called for minimum data security measures for all open banking participants, including authentication, authorization, encryption, and audit trails. On the operational side, the Final Report also called for enhanced IT security infrastructure, incident response monitoring, and penetration testing, among other measures.

While established financial institutions should be familiar with many if not all of these protective measures, these requirements may be cumbersome for smaller fintechs looking to become accredited and enter the system. Companies looking to utilize open banking to develop new fintech solutions should keep these data protections in mind early on in their development.

Liability

One important question in developing an open banking framework is which party is liable if financial data is accessed or disclosed without authorization. In its Final Report, the Committee suggested a simple concept that liability should "flow with the data" and rest with the party at fault. The Final Report called for a liability structure to prioritize consumer protection and redress, by requiring that the financial institution or third party service provider (as the case may be) pay out to the consumer immediately following their financial loss, and then work in collaboration with the corresponding party, or through alternative dispute resolution as needed, to seek compensation.[9]

The Final Report recommended that liability be aligned with provincial privacy legislation and guidance. Accordingly, open banking participants may wish to familiarize themselves with how Canadian privacy laws treat liability for breaches by organizations' service providers.

Consent

In its Final Report, the Committee called for specific rules around obtaining consumer consent. These include:

- a requirement for clear, simple and not misleading language;
- explanations of basic information such as what data is required, why such data is required, for how long it will be used, and possible risks of sharing that data;
- standardized consent processes; and
- a robust consent management system, such as a consent management dashboard.

These concepts are in keeping with current federal privacy legislation and guidance. When an organization collects sensitive information, PIPEDA generally requires express consent to be obtained,[10] and the OPC's guidelines on obtaining meaningful consent already require the same information noted above to be brought to consumers' attention in a clear, simple manner. Furthermore, organizations processing sensitive customer personal information are already required under applicable privacy laws to manage and record consent.

Transparency and Automated Decision Making

Since consumer trust is seen as fundamental to the success of an open banking system, transparency is a constant theme in the Final Report.[11] The Final Report calls for transparency in governance,[12] the

accreditation process,[13] and the liability structure (including the complaint process and rules for compensation when something goes wrong). As the Committee wrote, "[t]he rules should be clear, simple and enforceable so that all consumers, at all levels of financial literacy and vulnerability to cybersecurity threats, can clearly see they are protected while using the system."[14]

One open question is whether further transparency requirements will apply to automated decision making, and the use of algorithms. In its own submission to the Committee, the OPC called for more attention to be paid to the use of big data analytics and artificial intelligence by fintechs. The OPC noted that the lack of transparency in the manner in which automated algorithms are employed in an open banking model can pose difficulties for individuals wishing to access their information and challenge compliance.[15]

On the one hand, automated algorithms are typically proprietary, and may not be subject to open banking regulation. However, there is an idea developing in privacy law that consumers have a right to know about automated decisions that impact them. For example, Bill 64 will create a provision in Quebec's Private Sector Act requiring enterprises who make decisions based exclusively on automated processing of personal information to inform the person concerned of, among other things, the reasons and principal factors and parameters that led to the decision.[16] The proposed CPPA, before it died on the order paper, also contained a provision requiring organizations to make available a general account of their use of automated decision systems to make predictions, recommendations or decisions about individuals that could have significant impacts on them. The possible development of these rules is particularly relevant for automated investment management companies or similar third party robo-advisors.

Regulatory Powers of Enforcement

In its submissions to the Committee in February 2019, the OPC called for increased enforcement powers for itself, including the ability to make orders, impose fines, and conduct audits without grounds in order to keep organizations accountable.

Quebec's Bill 64 will provide the Quebec *Commission d'accès à l'information* ("**CAI**") with the authority to levy large fines of up to $10 million in penalties or an amount corresponding to 2% of the company's worldwide turnover, whichever is greater. The proposed CPPA also authorized fines up to the greater of $10 million or 3% of the organization's gross global revenue, as well as providing the OPC with the power to issue "Compliance Orders". If the federal government tables similar legislation to the CPPA, it is anticipated that it will include similar penalties and enforcement powers.

Conclusion

Though federal privacy law now staggers behind Quebec, many indicators point to a significant reform on the

horizon, in part due to developments relating to open banking. Financial institutions and third party fintechs should carefully monitor forthcoming privacy law developments, especially if they intend to participate in the open banking system in Canada.

If you have any questions about how to prepare for the regulatory changes relating to open banking in Canada, contact a member of our financial services group, or our privacy and data security group.

[1] Final Report, part 12 s.v. "Screen Scraping".
[2] Consumer-directed finance: the future of financial services.
[3] Office of the Privacy Commissioner of Canada, A Review into the Merits of Open Banking: Submission to the Department of Finance Canada.
[4] Final Report, part 5.4.
[5] Final Report, part 5.4.
[6] Bill 64, section 112.
[7] PIPEDA, Principle 4.7.
[8] Royal Bank of Canada v. Trang, 2016 SCC 50, at para 36.
[9] Final Report, part 7.1.
[10] PIPEDA, Principle 4.3.6.
[11] Final Report, part 1.
[12] Final Report, part 6.
[13] Final Report, part 8.
[14] Final Report, part 7.1.
[15] Office of the Privacy Commissioner of Canada, A Review into the Merits of Open Banking: Submission to the Department of Finance Canada, para 14.
[16] Bill 64, section 102.

by Darcy Ammerman, Mitch Koczerginski, Robbie Grant and Anthony Pallotta

A Cautionary Note

The foregoing provides only an overview and does not constitute legal advice. Readers are cautioned against making any decisions based on this material alone. Rather, specific legal advice should be obtained.