GDR NEWS

Canada's data privacy overhaul: the view from the provinces

28 October 2020

Canada's federal and provincial governments are modernising their data privacy frameworks – meaning virtually every private sector privacy statute is being rewritten. In the second of a two-article series, Dentons partner ***Kirsten Thompson*** *dissects proposed changes in British Columbia, Quebec and Ontario.*

Read the first article in the series, which covers changes at the federal level, here.

British Columbia

First published on the *Global Data Review* website, October 2020

ASpecial Committee of the Legislative Assembly was struck in February 2020 to review BC PIPA and has concluded public hearings and accepted written submissions. Its recommendations are expected in February 2021.

The review is happening in the context of proposed changes to PIPEDA and the implementation of the GDPR which, along with the content of the consultation submissions, provides hints about the topics that are likely to be addressed by the recommendations of the special committee:

Introduction of mandatory breach reporting: Although breach reporting has been mandatory in Alberta for a decade and came to PIPEDA in 2018, it is not currently required under BC PIPA. Harmonisation within Canada is a common theme in submissions and, given the trends, mandatory reporting is likely to be coming to BC.

Order-making power and the ability to impose penalties: The GDPR created significant enforcement measures and penalties for non-compliance. The privacy commissioners of Canada, Alberta and Ontario each advocated for the BC Privacy Commissioner to have enhanced order-making powers and the ability to issue administrative monetary penalties for BC PIPA breaches. This issue was the subject of similar recommendations in the special committee's previous report in 2016; it is expected that order-making powers will be recommended, and probably adopted.

Enhanced rights to control personal information, especially in light of new technologies: The value of personal information and the ability of organisations to process and analyse that information have increased massively since the original introduction of BC PIPA. The GDPR reflects this shift in its provisions about the right to data portability, the right to personal information erasure and clearer guidance about data de-identification and anonymisation. It is likely that the introduction of some of these rights will be recommended by the special committee, but which ones and to what extent is currently unclear.

Quebec

On 12 June 2020, the Quebec government proposed a significant overhaul of its current privacy laws through the introduction of Bill 64, 'An Act to Modernise

Legislative Provisions Respecting the Protection of Personal Information'. The changes proposed by Bill 64 go further than the changes being contemplated in other Canadian privacy laws – and in some respects, even further than those in the GDPR.

Bill 64 has been sent to the consultation stage at the Quebec National Assembly and will probably be amended. It seems unlikely that the changes proposed in Bill 64 would come into effect until 2022.

The key changes proposed are below.

Requiring consent for each specific purpose: Consent would be required for each specific purpose, in clear and simple language, and "separately from any other information provided to the person concerned". Bill 64 also requires express parental consent be obtained for those under the age of 14.

Establishing data governance and accountability mechanisms: Bill 64 mandates that all enterprises establish and implement governance policies and practices which must address certain things.

Requiring the designation of data protection officer: Enterprises would be required to designate a data protection officer, who would have to exercise "the highest authority" within the enterprise (although they can delegate this title to another personnel member in writing).

Requiring privacy impact assessments for all systems using personal data: Enterprises would be required to conduct "an assessment of the privacy-related factors of any information system project or electronic service delivery project involving the collection, use, communication, keeping or destruction of personal information". The scope of this requirement, and to what it might apply, is unclear at this time.

Mandating privacy by design: Enterprises which collect personal information "when offering a technological product or service" would be required to ensure the "highest level of confidentiality by default". However, it is currently unclear what enterprises would be considered as "offering a technological product or service".

First published on the *Global Data Review* website, October 2020

Right to erasure: This right would allow individuals to force enterprises to de-index hyperlinks or cease the dissemination of their personal information when such actions cause them "serious injury" in relation to reputation or privacy, subject to certain interests (.such as freedom of expression). If passed, this provision would require enterprises to develop internal processes for balancing such interests.

Right to request the source of information: Bill 64 would create the right to request the source of information where enterprises collect personal information from another person or entity.

Requirement for algorithmic transparency: Under the Bill, enterprises using personal information to render decisions based exclusively on automated processing must, at the time of or before the decision, inform the person concerned accordingly.

Opt-outs for profiling: The Bill would require anyone who collects personal information "using technology that includes functions allowing the person concerned to be identified, located or profiled" to first inform the affected person of the use of the technology, and the means available, if any, to deactivate those functions. This provision, if enacted, would, among other things, impose new obligations on the AdTech industry and users of such services.

Right to data portability: Bill 64 would require enterprises to provide individuals, on request, with personal information collected from the person in a structured, commonly used technological format. Note that this provision appears to apply only to electronic ("computerised") information and does not impose an obligation on an enterprise to digitise records in paper format.

Private right of action: Individuals could bring claims against enterprises for "injury resulting from the unlawful infringement of a right". Statutory punitive damages of at least C$1,000 (US$760) would be awarded when infringements are intentional or due to gross negligence.

Mandatory breach notification requirements: Under Bill 64, where a "confidentiality incident" presents a "risk of serious injury" to those impacted, the enterprise must "promptly notify"Quebec's data privacy regulator and affected individuals. Enterprises may also notify third parties that could reduce the

risk. Enterprises would also be required to maintain a register of confidentiality incidents.

New penalties for offences: Bill 64 gives more powers to the CAI, including the power to impose significant penalties. Enterprises face fines of up to C$25 million (US$19 million) or 4% of global turnover for the preceding fiscal year. Fines can be issued to enterprises that collect, hold, communicate to third parties or use personal information in contravention of the law; fail to report a breach; attempt to re-identify individuals without authorisation where their information is de-identified; impede investigations; or fail to comply with regulatory orders.

Ontario

On 13 August 2020, the Ontario government launched a consultation and released a discussion paper on the possible creation of a provincial private-sector privacy law. The government highlights several key areas for reform on which it is seeking input, specifically:

Opt-in for secondary uses of personal data: Enhanced consent requirement, including "an 'opt-in' model for secondary uses of information" (such as secondary marketing);

Right to erasure: A right for individuals to have their personal information deleted or de-indexed;

Alternatives to consent: The Ontario government has indicated it may consider basing the law on alternatives to consent. This would be tied to the requirement that organisations have clear and plain language information on their handling of personal information; organisations would then only seek consent for the processing of personal information other than that described in these notices. While this would reduce consumer friction, as a practical matter many businesses would be tied to PIPEDA's consent regime, so the impact of any Ontario provision will likely be minimal.

Penalty powers for the Ontario privacy commissioner: Added powers for the Ontario Information and Privacy Commissioner, including the power to impose penalties.

Carve-outs for de-identified data and derivative data: Specific restrictions and permitted uses for de-identified data and data derived from personal information.

Broad scope of application: The application of a new law to non-commercial activities (such as non-profits, charities, trade unions and political parties).

First published on the *Global Data Review* website, October 2020