SPECIAL COMMITTEE RELEASES REPORT SUGGESTING CHANGES TO MODERNIZE BC'S PRIVATE SECTOR PRIVACY LAW

Posted on December 15, 2021

Categories: Insights, Publications

The Special Committee to Review the *Personal Information Protection Act*[1] ("**PIPA**") released their report on December 6, 2021 (the "**Report**"), summarizing their recommendations to modernize PIPA.[2] In preparation of the Report, the Special Committee considered input and submissions from the Office of the Information and Privacy Commissioner of British Columbia ("**OIPC**") and other interested stakeholders over the past two years. In total, the Report makes 34 recommendations to modernize PIPA. In this bulletin, we will touch on a few notable recommendations to amend PIPA that may affect the processes and procedures of businesses governed by PIPA.

Meaningful Consent and Impacts of Emerging Technologies

Consent is central to PIPA – from explicit verbal or written consent to deemed or implicit consent – it represents the threshold of approval required from individuals to use their personal information. However, emerging technologies are challenging classic conceptions of privacy and consent. According to the Report, 67% of Canadians feel little to no control over how businesses use their personal information. To bridge this gap and allow businesses to properly collect and use personal information in a manner that provides individuals with a higher level of control, the Report recommends updating PIPA to include the concept of "meaningful consent".

For consent to be meaningful, the individuals must be fully aware of the nature of the personal information being collected, how it is collected, and what will be done with it. The Special Committee noted concerns about current privacy policies being overly complex and opaque. In particular, the Special Committee acknowledged concerns that privacy policies facilitate data collection through confusing language and allow over-collection of information. In light of the Special Committee's recommendation for inclusion of the concept of meaningful consent, businesses should be prepared to review and update their privacy policies to ensure that they are easily understandable by and accessible to an average person.

Further, new innovations and digital technologies such as the pervasive integration of mobile devices into daily activities, the proliferation of social media, and advancements in Artificial Intelligence ("**AI**") and biometrics can

challenge and have challenged the concepts of consent and choice, especially in the context of the processing of personal information. The Report recommends updating PIPA to require businesses who collect, use, disclose or otherwise process biometric data and other forms of sensitive personal information (such as political views, medical information, and information related to children and youth) to obtain explicit consent from the relevant individuals. The Special Committee also suggests that businesses collecting, using, disclosing or processing biometric data be required to reaffirm consent from individuals for such processes with reasonable frequency.

With respect to automatic decision-making systems and other forms of AI, the Special Committee recognizes the value that these technologies can offer on the one hand and the risk of algorithmic discrimination, re-identification, and violation of privacy on the other hand. The Special Committee notes that it is important to have appropriate regulation of AI in PIPA and recommends OIPC to undertake further studies (including public consultation) to understand the long-term socioeconomic impacts of AI in order to inform any proposed amendments to PIPA. Accordingly, the Report did not provide any recommendations concerning AI and automatic decision-making but asked that the OIPC provide proposed amendments to PIPA upon conclusion of the recommended further studies.

Finally, the Special Committee recommends broadening the definition of personal information in PIPA in order to address the heightened risk of re-identification of individuals' personal information as a result of the rapid growth in sophistication of technology. These changes would place pseudonymized data, or data that does not contain direct identifiers but is capable of re-identification, under the scope of consent requirements. For more information on the risks associated with anonymized and aggregated information, please refer to our bulletin here.

In discussing the above, the Report stressed the need to balance updating PIPA with increased consent requirements against the potential increased burden for both individuals and businesses. It remains to be seen how exactly this balance will be achieved through regulation, but it is expected that any changes to PIPA will place privacy protections along a spectrum, with the most sensitive information attracting the strongest protections.

Aligning PIPA with Canadian Privacy Legislation and the GDPR

In light of the proposed federal legislative changes to the *Personal Information Protection and Electronic Documents Act*[3] ("**PIPEDA**") introduced in Bill C-11 and the European Union's *General Data Protection Regulation*[4]("**GDPR**"), certain changes to PIPA may be required to ensure that PIPA remains "substantially similar" to PIPEDA and maintains adequacy with the GDPR. On the assumption that future legislation similar to Bill C-11 is reintroduced to amend PIPEDA, the Special Committee stressed the importance of PIPA

remaining in sync with PIPEDA and other similar provincial legislation. Consistency across legislative frameworks makes it easier for businesses to comply with various legislation and ensures that BC's economy and business sector remain competitive nationally and globally. As highlighted by the Report, BC's competitiveness in the marketplace is a key consideration for amendments to PIPA.

Aligning PIPA with other legislative frameworks will likely involve some material changes to PIPA. Most notably, the Report recommends the addition of mandatory breach notifications that would require organizations to promptly notify both the OIPC as well as affected individuals of a privacy breach, if the breach reaches a defined threshold. BC is currently the only province in Canada whose private sector privacy legislation does not require any mandatory notification in the event of a privacy breach.

The OIPC supports the introduction of mandatory breach notifications, stating that such notifications allow individuals to take steps to protect themselves if their personal information has or may have been compromised. The OIPC recommended that mandatory breach notifications be applied when the breach surpasses a "real risk of significant harm" threshold, meaning there is a real risk that the breach will lead to significant harm to the affected individual(s) considering the sensitivity of the breached information and the probability of the personal information has been, is being, or will be, misued. According to the OPIC, a "risk of significant harm" threshold would allow the OIPC to ensure that the most serious breaches are reported immediately.

With respect to these more serious breaches, businesses should be prepared for the introduction of fairly strict provisions including, for example, reporting privacy breaches within a short time period (for example, within 72 hours as required under the GDPR) and undertaking various methods of notification, including email, text, phone call and/or regular mail, to ensure individuals are informed. The OIPC also pushed for these provisions to be closely linked to increased administrative penalties, as discussed below.

The Report also discussed, among other issues, the introduction of the right to be forgotten and the right to data portability, both of which rights are enshrined in the GDPR. With respect to the right to be forgotten, the Special Committee notes that a more fulsome investigation of this right is required before any changes to PIPA be introduced. With respect to the right to data portability, the Special Committee recommends that businesses provide individuals with the right to obtain their own personal information in a machine-readable, transportable and commonly used format. This right would be separate from the right of an individual to obtain access to an individual's personal information and, if added to PIPA, businesses will likely need to implement new internal policies and revise their external facing privacy policies to ensure compliance with the amended PIPA.

Giving the OIPC "teeth"

The Report also suggests that the OIPC be given greater enforcement powers and that the amount of any fines which can be levied under PIPA be increased to act as a greater deterrent to violations of PIPA. If these recommendations are adopted, the OIPC will be able to:

- conduct audits to identify and investigate systemic issues, and issue findings and orders where there are reasonable grounds to do so;
- expand audits of private sector organizations;
- enter into compliance agreements with organizations, and require organizations to produce relevant reports upon request; and
- assess and issue fines directly against organizations who are found to be in violation of PIPA.

The Special Committee recognizes that the current administrative monetary penalties which can be assessed under PIPA are insufficient to act as a deterrent to potential violators. The Special Committee suggests adopting the principles of proportionality and scalability to address appropriately the impact of violations on the privacy of individuals and the impact of significant fines on businesses. However, the Committee members had diverging views regarding the appropriate amount of the fines. Some members proposed the amount of penalties be updated to account for inflation, which would be a fairly modest increase; whereas some other members would like the amount be increased to align more closely with the GDPR, which would be a much more significant increase.

Similar amendments regarding enforcement have been made to *BC's Freedom of Information and Protection of Privacy Act*, as discussed here, and *Ontario's Personal Health Information Protection Act*, as discussed here. Increased enforcement had also been included in Bill C-11, the proposed amendments to the federal private sector privacy laws, as discussed here. As such, changes relating to increased enforcement and penalties are likely to be adopted in any amendments coming to PIPA.

Conclusion

It remains to be seen what recommendations may be adopted by the British Columbia Legislature, but it seems that based on trends in privacy legislation across Canada that many of these changes are likely to be implemented. If you have any questions regarding how these changes may impact your business, we recommend you reach out to our Privacy and Cybersecurity Group.

[1] SBC 2003, c. 63.
[2] British Columbia, Legislative Assembly, Special Committee to Review the Personal Information Protection Act, *Modernizing British Columbia's Private Sector Privacy Law*, 42nd Parl, 2nd Sess (6 December 2021) (Chair: Mable Elmore).

[3] SC 2000, c 5.
[4] (EU) 2016/679.

by Robert Piasentin, Gurp Dhaliwal, Yue Fei and Kristen Shaw (Articled Student)

A Cautionary Note