THE CANADIAN BAR ASSOCIATION
British Columbia Branch

October 21, 2019

MATT REED Via email: Matt.Reed@gov.bc.ca
Executive Director, Privacy, Compliance and Training
Ministry of Citizens' Services
PO Box 9406 Stn. Prov. Govt.
Victoria BC V8W9V1

Dear Mr. Reed,

RE: SECTION 22 OF THE *MISCELLANEOUS STATUTES AMENDMENT ACT (NO. 2)* (BILL 35) AMENDING SECTION 33.1(1)(p) AND ADDING (p.1) AND (p.2) OF THE *FREEDOM OF INFORMATION AND PROTECTION OF PRIVACY ACT*

We are writing on behalf of the Canadian Bar Association (British Columbia Branch) ("CBABC") Freedom of Information & Privacy Law Section (the "Section") regarding proposed amendments to section 33.1(1)(p) and addition of paragraphs (p.1) and (p.2) of the *Freedom of Information and Protection of Privacy Act*[1] made by section 22 of the *Miscellaneous Statutes Amendment Act (No. 2), 2019* (Bill 35).[2]

CBABC

Formed in 1896, the purpose of the CBABC is to:

- Enhance the professional and commercial interests of our members;
- Provide personal and professional development and support for our members;
- Protect the independence of the judiciary and the Bar;
- Promote access to justice;
- Promote fair justice systems and practical and effective law reform; and
- Promote equality in the legal profession and eliminate discrimination.

The Canadian Bar Association nationally represents approximately 35,000 members and the British Columbia Branch itself has over 7,000 members. Our members practice law in many different areas. The CBABC has established 76 different sections to provide a focus for lawyers who practice in similar areas to participate in continuing legal education, research and law reform. The CBABC has also established standing committees and special committees from time to time.

[1] See http://canlii.ca/t/8421.

[2] See https://bit.ly/32uYtaa.

CBABC Freedom of Information & Privacy Law Section

The CBABC Freedom of Information & Privacy Law Section provides a forum for the exchange of information, networking and education of lawyers practising or interested in the area of freedom of information and privacy law. The Section is comprised of members who work in, or represent clients from, diverse sectors including industry, public interest organizations, public bodies, and privacy and freedom of information advocacy organizations.

The Section was assisted in the preparation of this letter submission by Stuart Rennie, CBABC Legislation and Law Reform Officer.

The Section's submissions in this letter reflect the views of the members of the Section only and do not necessarily reflect the views of the CBABC as a whole.

Submissions

1. The proposed amendment to s. 33.1(1)(p) and addition of paragraphs (p.1 and p.2) of the *Freedom of Information and Protection of Privacy Act* ("FIPPA") are intended to repeal and replace a paragraph to address grammar, clarity and redundancy, and add authority for the limited disclosure of personal information inside or outside Canada for temporary information processing not involving intentional access by an individual, involving metadata only, or if certain conditions are met.

2. To the extent that the Bill 35 amendments are designed to permit BC public bodies to engage with cloud-based service providers with Canadian-based infrastructure, we support the proposed amendments to s. 33.1.

3. However, we take the opportunity to comment on ss. 30.1 and 33.1 beyond what is contemplated in the proposed amendments and to reiterate the relevant recommendations made by the Section in the past.

4. Our Section has previously made submissions respecting the data sovereignty requirement contained in section 30.1 of FIPPA, in 2016[3] and in 2018[4].

5. In each submission, our Section recommended that the legislation be amended to give public bodies the discretion to disclose, access and store personal information outside Canada in limited circumstances which are transparent, reviewable, and

[3] Submissions of the CBABC to the Special Committee to Review FIPPA, January 14, 2016; see pages 6 to 14, https://bit.ly/32oC4LV.

[4] Submissions of the CBABC to the BC Ministry of Citizens' Services Regarding Practices Under FIPPA, April 9, 2018; see pages 12 to 16, https://bit.ly/2IZw8kK.

where the benefit of doing so clearly outweighs the potential harm. We reiterate that recommendation here.

6. In 2016, the BC Legislative Assembly's Special Committee acknowledged and agreed with the government that it should continue to monitor changes in privacy laws and in technology solutions to ensure that section 30.1 remains relevant and practical.

7. Since that time, cloud-based storage and software applications have only become increasingly prevalent, and necessary for public bodies to provide goods and services to the public. Companies such as Microsoft, Adobe and Amazon have been working to establish cloud-based storage and applications based in Canada. Smaller service providers offer an increasing range of cloud-based services and niche applications; however few have the resources necessary to establish Canadian-based storage and processing facilities. Notably, regulators have raised questions over whether even the Canadian-based operations are sufficiently beyond the reach of foreign governments to satisfy the requirements of section 30.1 of FIPPA.

8. We reiterate the observations that our Section made in 2016 and 2018 regarding the negotiated transborder flow of information between the European Union ("EU") and the US under the Privacy Shield. Specifically, we note that the EU's General Data Protection Regulation ("GDPR") contemplates transborder flows of personal information where sufficient guarantees of security are present (i.e., where a non-member country achieves adequacy status or where another permissible structure for information transfer is in place)[5]. The GDPR has adopted a more flexible approach to transborder data flows than FIPPA, notwithstanding the fact that the GDPR is arguably a more prescriptive piece of legislation from a privacy protection perspective than FIPPA.

9. In light of these observations, our Section agrees that it is appropriate at this time for our government to revisit FIPPA's data sovereignty provisions to ensure that they continue to be relevant and practical. This includes revision not only of transborder disclosure requirements, but storage and access as well.

10. The proposed Bill 35 amendments partially address what we submit is a current gap between the scope of section 30.1 and the practical requirements of transborder information flow by broadening the scope of extraterritorial access. The intent of the amendments appears to be to permit public bodies to meet the requirements of cloud-based service providers with Canadian-based storage infrastructure.

11. To the extent that these revisions are drafted to allow public bodies to engage more directly with the software service options available in the modern world, our Section supports the amendments. However, in our submission, even the revised language

[5] *Supra* footnote 3 at p. 11; *Supra* footnote 4 at page 12.

would continue to significantly restrict public bodies by preventing extraterritorial information storage.

12. We are mindful of the fact that many, if not all, public bodies have as their mandate the delivery of services that are also designed to serve some aspect of the public good. As a matter of practical reality, even the amended section 33.1 would restrict those public bodies to engaging with a small handful of the largest cloud-based service providers, who have the resources to develop the necessary Canadian-based infrastructure. In our submission, this will likely result in negative service cost consequences for BC's public bodies, and restrict their access to the growing body of cloud-based services, specifically those that offer stronger reasonable security arrangements and privacy protections, particularly where the personal information at issue is not highly sensitive.

13. As noted, this restriction is more onerous than other regimes that employ a high degree of privacy protection. In addition, it is unclear whether even Canadian-based cloud computing service providers are or will remain sufficiently beyond the reach of foreign governments to satisfy the goal of restricting extraterritorial storage. Given the rapid evolution of cloud-based technology, our submission is that a continued blanket restriction on extraterritorial storage significantly restricts the province's public bodies without necessarily ensuring continued privacy protection in a changing environment.

14. We emphasize that we do not propose to place administrative expedience above the protection of the privacy of citizens of BC, nor should our submissions be read as such. Rather, we are mindful of the fact that public bodies may be prevented or undermined in their attempts to fulfill their public mandate while also protecting personal information in the best manner possible by legislative restrictions that are overbroad and that, in the end, may not be particularly effective in achieving the ends they were designed to achieve.

15. As an alternative to a continued blanket restriction on extraterritorial storage, we submit that one way to address the concerns associated with transborder information flow would be to introduce a more nuanced analysis into section 30.1.

16. A nuanced analysis would include a risk assessment of the nature of the information to be stored or accessed, the destination of the information and the legal recourse that may be available to a BC citizen in that foreign destination, or the (non)-existence of available and appropriate alternatives within Canada. An analysis of the nature and sensitivity of the information involved could draw on, for example, a similar scrutiny to that outlined in section 22 of FIPPA. Additional risk factors to be assessed could also include the strength of the safeguards in place for the storage or access.

17. This approach would align our province with other Canadian jurisdictions that have adopted legislation which specifically contemplates and controls transborder information flow. For example, the Nova Scotia *Personal Information International Disclosure Protection Act* permits a public body to authorize extraterritorial access and storage, but requires that it report such access or storage to the Minister of Justice and explain the reason it has been determined necessary.[6] This legislation also requires an examination and determination of the conditions of storage or access, and provides a transparent system whereby the public body's decision is recorded and subject to review.

18. Introducing similar nuance to FIPPA would not, in our respectful submission, negate all of the protection that the legislation currently offers. To the contrary, if BC were to adopt an approach similar to that described above, the government could actually enhance public body accountability by making data flows more transparent, while allowing public bodies to access a greater range of the available software services. The government could do so by requiring publication annually of the public body's decision to allow storage or access outside Canada, the conditions or restrictions that have been applied to such transborder storage or access, and a statement of precisely how the transborder storage or access meets the necessary requirements of the public body's operations. This would provide the public with transparent access to how their information is being handled by public bodies in transborder data flows.

19. We acknowledge the comments made by the Information and Privacy Commissioner for British Columbia ("OIPC") regarding Bill 35 by way of letter titled "Bill 35—Miscellaneous Statutes Amendment Act (No. 2), 2019; OIPC File F19-80600", dated October 9, 2019.[7] At this time, due to time constraints in preparing the Section's submissions, our efforts to keep the submissions brief, and the technical nuances of certain terminology included in the proposed amendments, the Section has refrained from commenting on the specific language in the proposed amendments and on the recommendations of the OIPC, and has kept its submissions more general in nature. However, given the opportunity, we look forward to providing additional input regarding these considerations.

Conclusion

In conclusion, the Section makes the following comments and recommendations:

1. To the extent that the Bill 35 amendments are designed to permit BC public bodies to engage with cloud-based service providers with Canadian-based infrastructure, we support the proposed amendments to section 33.1.

[6] See http://canlii.ca/t/lcp7.

[7] See https://www.oipc.bc.ca/public-comments/2343.

2. We continue to recommend further amendments to the legislation to permit storage of personal information outside of Canada, where the benefit of doing so clearly outweighs the potential harm. We recommend that such amendment allow public bodies to make a nuanced analysis of the nature of the information, the destination of the information, legal and technical safeguards in place, available legal recourse in the foreign destination and the availability of appropriate alternatives within Canada, and create a transparent system whereby the public body's decision is recorded and subject to review.

The Section is pleased to discuss our submissions further, either in person or in writing, in order to provide any clarification or additional information that may be of assistance.

Communications in this regard can be directed to:

SINZIANA M. GUTIU
Co-Chair, CBABC Freedom of Information & Privacy Law Section
Tel.: (778) 689-2537
Email: Sinziana.Gutiu@telus.com

KELLY A. SAMUELS
Co-Chair, CBABC Freedom of Information & Privacy Law Section
Tel.: (604) 661-1003
Email: ksamuels@ekb.com