SUBMISSIONS OF THE CANADIAN BAR ASSOCIATION (BRITISH COLUMBIA BRANCH)

TO THE

BC MINISTRY OF CITIZENS' SERVICES

REGARDING **PRACTICES** UNDER THE

FREEDOM OF INFORMATION AND PROTECTION OF PRIVACY ACT

Issued By:

Canadian Bar Association
British Columbia Branch

Special Committee of the
Freedom of Information and
Privacy Law Section

April 9, 2018

Table of Contents

PREFACE

Formed in 1896, the purpose of the Canadian Bar Association (British Columbia Branch) (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 CBA nationally represents approximately 35,000 members and the British Columbia Branch itself has over 6,500 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.

The Freedom of Information and Privacy Section of the CBABC (the "Section") is comprised of members of the CBABC who share an interest or practice law in areas that pertain to freedom of information and privacy issues generally. The following submissions reflect the views of individual Section members, and not necessarily the views of the CBABC or the Section as a whole.

EXECUTIVE SUMMARY

Section members submitted comments in relation to 8 matters. First is solicitor client privilege. Second is mandatory breach reporting. Third is data localization. Fourth are employment investigations. Fifth is technological neutrality. Sixth is the possibility of modified timelines. Seventh is the possibility of strengthened protections for confidential business information and trade secrets. Eight is the lawyer as a representative under FIPPA. Some members proposed specific recommendations and these recommendations are summarized at the end of our submissions.

SUBMISSIONS

The Section is pleased to respond to the request for submissions from the Ministry regarding the Ministry's consultation regarding how effective are practices under the *Freedom of Information and Protection of Privacy Act* (FIPPA). The Ministry created a website regarding this FIPPA consultation, available here.

The Section's submissions are organized around 8 matters:

1. Solicitor client privilege.
2. Mandatory breach reporting.
3. Data localization.
4. Employment Investigations.
5. Technological neutrality.
6. Possibility of modified timelines.
7. Possibility of strengthened protections for confidential business information and trade secrets.
8. Lawyer as "representative" under FIPPA.

SOLICITOR CLIENT PRIVILEGE

In January 2016, a Special Committee of the Section filed written submissions with the BC Legislative Assembly's Special Committee to review FIPPA (the "2016 Section Submissions").[1] In these submissions, the Section made comment about the operation of section 25. Section 25 of FIPPA requires that specified information must be disclosed if it is in the public interest. In our 2016 submissions, the Section pointed out concerns that interpretations of section 25 could weaken the protections around solicitor client privilege.[2]

The importance of solicitor-client privilege to our justice system cannot be overstated. It is a legal privilege concerned with the protection of a relationship that has a central importance to our system as a whole.

Without the assurance of confidentiality, people cannot be expected to speak honestly and candidly with their lawyers, which compromises the quality of the legal advice they receive.

Solicitor-client privilege is not now a mere privilege under the law of evidence. In jurisprudence developed over the last 20 years, the Supreme Court of Canada has articulated that solicitor-client privilege has acquired constitutional dimensions.[3]

---

[1] See https://www.cbabc.org/Our-Work/Submissions/2014/Submission-to-the-Legislative-Assembly-of-British

[2] Pages 30-32.

[3] *Alberta (Information and Privacy Commissioner) v. University of Calgary*, [2016] 2 SCR 555, 2016 SCC 53 (CanLII), http://canlii.ca/t/gvskr at para. 20.

The Information and Privacy Commissioner for BC has recognized the right of public bodies to claim solicitor-client privilege, litigation privilege and common interest privilege as follows:

a) Solicitor-Client Privilege: The Board of Education of School District 71 (ComoxValley), Order F15-67 (December 3, 2015);[4]

b) Litigation Privilege: Ministry of Health Order F15-41 (August 21, 2015);[5] and

c) Common Interest Privilege: Victoria Police Department Order F15-61 (November 10, 2015).[6]

Some Section members argue that section 25 will apply despite any other provision of FIPPA; the fact that another provision of FIPPA applies should be a factor to consider when weighing whether the public interest militates in favour of disclosure. In other words, it should be made clear that solicitor-client privilege should first be considered as a factor when weighing whether public interest militates in favour of disclosure.

---

[4] See 2015 BCIPC 73 (CanLII), http://canlii.ca/t/gmpx6

[5] See 2015 BCIPC 44 (CanLII), http://canlii.ca/t/gkxmq

[6] See 2015 BCIPC 67 (CanLII), http://canlii.ca/t/gmbhj

The various Information and Privacy Commissioners across Canada have drafted a resolution calling for general amendments to legislation where there is ambiguity to expand the Information and Privacy Commissioner for BC's powers to review solicitor-client privileged documents.

The challenge here is that the Information and Privacy Commissioner for BC acts as both adjudicator and advocate. This creates a situation where the Information and Privacy Commissioner for BC could be compelling disclosure of legal advice about a situation where the advice is that the Commissioner has interpreted an issue in a way that is incorrect or, for example, contrary to law in another jurisdiction. Some members of the CBABC submit that public bodies should not be compelled to disclose solicitor-client privileged information that could, by its very nature, put the public body into a position that is contrary to the Information and Privacy Commissioner for BC's role as an advocate.

Accordingly, we respectfully submit that any amendments to FIPPA should serve to respect and protect solicitor-client privilege. We also submit that, it should be made clear that solicitor-client privilege should first be considered as a factor when weighing whether public interest militates in favour of disclosure under section 25.

MANDATORY BREACH REPORTING

Currently, FOIPPA does not provide specific language that requires notification to affected individuals and the Information and Privacy Commissioner for BC. The Information and Privacy Commissioner for BC has taken the position that mandatory breach reporting is implicitly part of a public body's obligation to safeguard personal information under section 30 of FIPPA.

In our 2016 Section Submissions, we provided detailed recommendations for the addition of mandatory breach notification as follows:

a) Creation of a new section 36.2 and a new Division 4 in Part 3 of FIPPA that is similar to Alberta's *Personal Information Protection Act* (PIPA) in section 34.1 regarding notification to the Information and Privacy Commissioner for BC;

b) Creation of a new section 44.3 similar to Alberta's PIPA section 37.1, expanding the "powers of commissioner in conducting investigations, audits or inquiries" to allow the Information and Privacy Commissioner for BC to investigate any breaches arising from the proposed section 36.2;

c) Creation of a new Schedule 4 similar to Alberta's PIPA Schedule 4 providing details on the form and content of the notification to individuals and the Information and Privacy Commissioner for BC.[7]

[7] See pages 32 to 41.

The Section submits that our recommendations in our 2016 Section Submissions are still valid.

British Columbians often do not have a choice when it comes to providing their personal information to public bodies for many essential public-sector services such as health, transit, car insurance, hydro/electricity and education. Mandatory breach notification is therefore important to ensure that their information is protected and British Columbians are not left in the dark when their personal information is negatively affected as a result events like snooping or inadequate privacy safeguards.

BC is falling behind personal information protection acts in other provinces, federally and internationally. Some examples include:

a) Ontario's *Personal Health Information Protection Act* provides strict breach notification requirements to the Ontario Privacy Commissioner, appropriate Colleges, and affected individuals;[8]

b) Nova Scotia's *Personal Health Information Act* includes mandatory breach reporting by custodians to affected individuals if there is potential for harm or embarrassment;[9]

[8] See *Personal Health Information Protection Act, 2004*, S.O. 2004, c. 3, Sch. A, http://canlii.ca/t/53154

[9] See *Personal Health Information Act*, S.N.S. 2010, c. 41, http://canlii.ca/t/52pkj

c) Alberta's PIPA requires mandatory breach reporting where there is a real risk of significant harm;[10]

d) Canada's *Personal Information Protection and Electronic Documents Act* has now been amended to include provisions that (once in force) will require breach notification;[11]

e) European Union's General Data Protection Regulation (GDPR) has strict mandatory breach reporting requirements with serious penalties for non-compliance; and[12]

f) in the United States, all 50 states, the District of Columbia, Guam, Puerto Rico and the Virgin Islands have enacted legislation requiring private or governmental entities to notify individuals of security breaches of information involving personally identifiable information.[13]

[10] See *Personal Information Protection Act*, S.A. 2003, c. P-6.5, http://canlii.ca/t/53322

[11] See *Personal Information Protection and Electronic Documents Act*, S.C. 2000, c. 5, http://canlii.ca/t/52hmg

[12] See https://www.eugdpr.org/

[13] See National Conference of State Legislatures, http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx

DATA LOCALIZATION

In 2016, following receipt of submissions from many stakeholders, including our 2016 Section Submissions, the Information and Privacy Commissioner for BC, BC Freedom of Information and Privacy Association and the BC Civil Liberties Association, the BC Legislative Assembly's Special Committee recommended in its report that the data sovereignty requirement contained in section 30.1 of FIPPA should be retained.

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

This recommendation and these comments were issued at a time when the European Court of Justice had just recently issued a decision invalidating US Safe Harbour. It was also a time when companies such as Microsoft, Adobe and Amazon were working to establish cloud-based storage and software applications that would be based in Canada.

Subsequently, the European Union (the "EU") and the US have negotiated the terms of the Privacy Shield, although that instrument may itself be subject to legal challenge under the GDPR. That said, the negotiation of the Privacy Shield demonstrates the need and willingness of EU member states to permit the transborder flow of personal information to the US, provided that appropriate protections are in place.

Perhaps more importantly for our context, the fact that the GDPR does contemplate such transborder flows of personal information where a non-member country, such as Canada, achieves adequacy status, or where other permissible vehicles for transferring personal information (e.g. binding corporate rules, or standard form contracts) are employed, demonstrates that the GDPR has adopted a more flexible approach to transborder data flows than does FIPPA. This is the case despite the fact that the GDPR is arguably a far more privacy-protective piece of legislation than FIPPA.

In the meantime, while some of the promised Canada-based cloud storage and software applications has come to pass, regulators have nevertheless raised questions over whether these Canadian-based operations are sufficiently beyond the reach of foreign governments to satisfy the requirements of section 30.1 of FIPPA.

The Section submits that in light of these developments, it is an ideal time for the BC government to revisit FIPPA's data sovereignty provisions to ensure their continued relevance and practicality.

Back in 2016, our 2016 Section Submissions recommended that section 30.1 of FIPPA be amended to give public bodies the discretion to store or access personal information outside Canada under limited circumstances where the benefit of doing so clearly outweighs the potential harm.[14] To do so would enable public bodies to perform their

[14] See pages 6 to 14.

mandates more effectively, in the spirit of FIPPA, and would ensure compliance with international standards and treaty obligations. We reiterate that recommendation here.

We do not intend this submission as an argument placing administrative expedience above the protection of the privacy of citizens of BC, nor should it be read as such. Rather, 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, but are being prevented or undermined in their attempts to fulfill this mandate 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. For example, the application of section 30.1 of FIPPA to personal information held by public bodies in B.C. lacks nuance, in that it involves no 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.

To introduce such nuance to section 30.1 would not, in our respectful submission, negate all of the protection that section 30.1 currently offers. To the contrary, if BC were to adopt the approach taken by Nova Scotia in its *Personal Information International Disclosure Protection Act*, the B.C. government could actually hold public bodies more accountable, and make their transborderdata flows more transparent.[15] The BC

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

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 transborderstorage or access, and a statement of precisely how the transborderstorage or access meets the necessary requirements of the public body's operations.

EMPLOYMENT INVESTIGATIONS

In our 2016 Section Submissions, we pointed out the inconsistency in treatment of direct and indirect collection of employee information for the purposes of managing or terminating an employment relationship under sections 27(1)(f) and 27(4) of FIPPA.[16]

In our 2016 Section Submissions, we explained how the negative impact of this inconsistency operates in notification requirements, and we recommended amending FIPPA to permit a public body to not notify the employee that it is collecting personal information, either indirectly or directly, where it is reasonable that such notification would compromise the availability or accuracy of information, or would compromise an investigation or a proceeding related to the employment of the employee.

As well, in the May 2016 Report of the BC Legislative Assembly's Special Committee to Review the *Freedom of Information and Protection of Privacy Act,* the Special

[16] Pages 32 to 34.

Committee also recommended amending FIPPA to permit a public body to not notify an employee that it is collecting their personal information, either indirectly or directly, for the purpose of managing or terminating the employment relationship, where it is reasonable to expect that doing so would compromise (a) the availability or the accuracy of the information, or (b) an investigation or a proceeding related to the employment of the employee.[17]

This strange inconsistency in notification requirements depending on whether the collection is direct or indirect – which does not exist in the *Personal Information Protection Act* -- can make it impossible for public bodies to conduct an effective investigation. For example, when investigating an allegation of serious wrongdoing by an employee, the employer does not have to notify the employee before it interviews witnesses (because this is indirect collection) but it does have to notify the employee that the employer will be reviewing the employee's Internet logs (because this is direct collection) – even if by doing so, the employee will have an opportunity to tamper with the evidence and thereby compromise the availability or accuracy of the information.

FIPPA has not been amended in this way as we recommended since we made our 2016 Section Submissions. We submit our 2016 recommendations in this regard are still valid.

[17] See https://www.leg.bc.ca/content/committeedocuments/40th-parliament/5th-session/foi/report/scfippa_report_2016-05-11.pdf

Some Section members also note that the fact that work product is not expressly exempted from the definition of personal information in FIPPA causes confusion and uncertainty on a day-to-day basis in the employment relationship, but also when responding to access requests. As a result, we recommend that FIPPA be amended to expressly carve out "work product" from the definition of "personal information" listed in Schedule 1 of FIPPA.

TECHNOLOGICAL NEUTRALITY

To prevent privacy laws from being circumvented by technological advancements, the Section recommends that FIPPA remain technology-neutral.

Recital 15 and 27 and Article 3 of the European Union's Data Protection Directive (95/46/EC)[18] and Recital 15 and Article 2(1) of the GDPR expressly provide for technological neutrality by stating that protections for individuals should not depend on the techniques used.

We recommend that FIPPA likewise remain technologically neutral. This can be done by expressly including a provision in Division 1 like in the Data Protection Directive and the GDPR to clarify that the protections in FIPPA are technologically neutral.

[18] See http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:31995L0046&from=EN

To avoid ambiguity in FIPPA, it may be helpful to clarify in FIPPA that "technological neutrality" refers to privacy protections that are not technology-specific by:

a) Focusing on the intended effect of the protection and providing flexibility in the means of achieving the effects;

b) Regulating behaviour of people or public bodies who have custody or control of personal information as opposed to that of specific types of machines or algorithms; and

c) Regulating the use or design of technology as opposed to the technology itself.

We recommend that FIPPA be amended to add an express provision regarding technology to ensure that FIPPA is always applied in a manner that survives the ever-changing landscape of technological innovation.

POSSIBILITY OF MODIFIED TIMELINES

We have been asked to consider the idea of staggered timelines for responses to access requests, including (1) having different timelines for individual as opposed to business applicants, or (2) having different timelines for B.C. and non B.C. residents. We recommend that the timelines under FIPPA remain as they are at this time. Section members identified numerous issues with applying different timelines on the basis of location and/or on the basis of being an individual or a company.

Definition of "individual" versus "business"

One issue is how "business" would be defined. Would "business" include only corporations? Would it include non-profits? Would it include unions? Political parties? News organizations? Volunteer groups? Advocacy groups? On what basis would some groups be included and others not?

Distinguishing between individuals and "businesses" (however they might be defined) implies that the business' purpose may be inherently less legitimate than a request made by an individual. Some members submit that it is a fundamental principle of access to information law that the purpose of the applicant's request is irrelevant and that it is not for the public body to determine whether or not they approve of what the applicant might use the information for.

Ease of avoiding longer timelines

Some members pointed out that differences in response timelines on the basis of identity and/or location could easily be avoided as any business that wanted to take advantage of a shorter time line could file an application for access to information through an individual representative (or legal counsel) located in British Columbia. If differential timelines applied to individuals (and not just business) outside of BC, this has the potential of creating a two-tiered system by which individuals who have access to a BC address (family, friends, legal counsel) could take advantage of a "Resident's

timeline" but those without family, friends, or money for counsel would be treated differently.

Undermining quasi-constitutional right

Perhaps most importantly, differential treatment in an arbitrary manner has the potential to undermine the quasi-constitutional nature of privacy and access laws, and their purpose of facilitating democracy. As Mr. Justice La Forest of the Supreme Court of Canada stated in *Dagg v. Canada (Minister of Finance):*

> The overarching purpose of access to information legislation, then, is to facilitate democracy. It does so in two related ways. It helps to ensure first, that citizens have the information required to participate meaningfully in the democratic process, and secondly, that politicians and bureaucrats remain accountable to the citizenry. As Professor Donald C. Rowat explains in his classic article, "How Much Administrative Secrecy?" (1965), 31 *Can. J. of Econ. and Pol. Sci.* 479, at p. 480:
>
> > Parliament and the public cannot hope to call the Government to account without an adequate knowledge of what is going on; nor can they hope to participate in the decision-making process and contribute their talents to the formation of policy and legislation if that process is hidden from view.[19]

As such, we respectfully submit that distinguishing between an individual and "a business", or distinguishing between applicants on the basis of location, is contrary to the object of the legislation.

In addition, we recommend that current timelines for responding to access requests remain as they are at this time.

[19] [1997] 2 SCR 403, 1997 CanLII 358 (SCC), http://canlii.ca/t/1fr0r at para. 61.

POSSIBILITY OF STRENTHENED PROTECTIONS FOR CONFIDENTIAL BUSINESS INFORMATION AND TRADE SECRETS

Some members submit that the limits on disclosure that FIPPA currently contains, including for confidential business information and trade secrets, permit public bodies to extend timelines for the purposes of getting third party input, and go some way towards reducing the incentives for businesses to use freedom of information law to gain access to the sensitive commercial information of their competitors. It is in the public interest for governments to be transparent. Some members argue that it is in the public interest for contracts to be released, including pricing and other competitive information since it is tax dollars that are being expended on such contracts.

However, some Section members would like to see better protections for confidential business information and trade secrets. Some members submit that the potential for this type of information to be disclosed has actually made some businesses decide against working with public bodies. Some members describe some people and companies using the access process to intentionally obtain pricing, trade secrets and other commercially sensitive information from competitors, or to force competitors who won a bid to needlessly expend resources responding to requests rather than focus on their business. The consequence of such tactics is that some companies price in these costs to their bids on public contracts, which raises the prices of the goods and services supplied to governments, while others decide to not risk exposure of their commercially sensitive information and self-select out of the bid process. Some members submit these tactics discourage competent businesses from wanting to engage in Requests

For Information, Request For Proposals and negotiations with the government, leading to a smaller pool of service providers; and unintentionally leading to a less competitive market for governments and the taxpayers who fund them. As a result, some Section members argue that it would be in the public interest to work to get those protections strengthened.

Some Section members argue that the threshold for denying access to procurement/contract information when there is evidence of harm to the public body or its service provider(s) may be too low. This may be addressed by strengthening the provisions under sections 17 and 21 of FIPPA and in particular by examining the current interpretation of section 21(1)(b).

LAWYER AS REPRESENTATIVE UNDER FIPPA

Some Section members have requested that FIPPA be amended to add “a lawyer” to the list of representatives who may access private information on behalf of an individual under section 4(1) of the Regulation. Some members submit that, for example, in the corrections environment, requiring a signed written consent form before legal counsel may obtain client documents from B.C. Corrections imposes an unnecessary administrative burden and in some cases unnecessary delay in dealing with issues such as solitary confinement, which engages liberty rights under section 7 of the Charter.

Lawyers are obliged to act in accordance with professional ethics and standards of conduct set out in the *Legal Profession Act*, the Law Society Rules and the Code of Professional Conduct for British Columbia. Clients would be protected from any potential misconduct posed by this amendment by the complaint and disciplinary procedures of the Law Society of British Columbia.

LIST OF RECOMMENDATIONS

SOLICITOR CLIENT PRIVILEGE

1.We recommend clarifying that that solicitor-client privilege should first be considered as a factor when weighing whether public interest militates in favour of disclosure.

2.We also recommend that any amendments to FIPPA ensure respect for and protection of solicitor-client privilege.

MANDATORY BREACH REPORTING

3. We recommend, as we stated in our 2016 Section Submissions, that FIPPA be amended to:

a) Create a new section 36.2 and a new Division 4 in Part 3 of FIPPA that is similar to Alberta's *Personal Information Protection Act* (PIPA) in section 34.1 regarding notification to the Information and Privacy Commissioner for BC;

b) Create a new section 44.3 similar to Alberta's PIPA section 37.1, expanding the "powers of commissioner in conducting investigations, audits or inquiries" to allow the Information and Privacy Commissioner for BC to investigate any breaches arising from the proposed section 36.2;

c) Create a new Schedule 4 similar to Alberta's PIPA Schedule 4 providing details on the form and content of the notification to individuals and the Information and Privacy Commissioner for BC.

DATA LOCALIZATION

4. We recommend, as we stated in our 2016 Section Submissions, that FIPPA be amended in section 30.1 to give public bodies the discretion to store or access personal information outside Canada under limited circumstances where the benefit of doing so clearly outweighs the potential harm. If BC were to adopt the approach taken by Nova Scotia in its *Personal Information International Disclosure Protection Act*, the B.C. government could actually hold public bodies more accountable, and make their transborderdata flows more transparent. The BC 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 transborderstorage or access, and a statement of precisely how the transborderstorage or access meets the necessary requirements of the public body's operations.

EMPLOYMENT INVESTIGATIONS

5. We recommend, as we stated in our 2016 Section Submissions, that FIPPA be amended to permit a public body to not notify the employee that it is collecting their personal information, either indirectly or directly, where it is reasonable to expect that doing so would compromise (a) the availability or the accuracy of the information, or (b) an investigation or a proceeding related to the employment of the employee.

6. We recommend that FIPPA be amended to expressly carve out "work product" from the definition of "personal information" in Schedule 1.

TECHNOLOGICAL NEUTRALITY

7. We recommend that FIPPA remain technologically neutral, by expressly including a provision in Division 1 like in the Data Protection Directive and the GDPR to clarify that the protections in FIPPA are technologically neutral.

TIMELINES

8. We recommend that the FIPPA timelines should remain as they are.

SENSITIVE COMMERCIAL INFORMATION AND TRADE SECRETS

9. We recommend considering how to strengthen protections in respect of sensitive commercial information and trade secrets. This may be addressed by addressing the threshold for disclosure where there is evidence of harm to the public body and/or its service providers.

LAWYER AS "REPRESENTATIVE" UNDER FIPPA

10. We recommend that section 4 of FIPPA be amended to add "a lawyer" to the list of representatives who may access private information on behalf of an individual.

CONCLUSION

We would be pleased to discuss our submissions further with the Ministry, either in person or in writing, in order to provide any clarification or additional information that may be of assistance to the Ministry.

Communications in this regard can be directed to:

KERI L. BENNETT
Co-Chair, CBABC Freedom of Information & Privacy Law Section
Tel.: (604) 806-3848
Email: kbennett@ropergreyell.com

J. ALEXIS KERR
Co-Chair, CBABC Freedom of Information & Privacy Law Section
Tel.: (604) 587-4671
Email: Alexis.Kerr@fraserhealth.ca