SUBMISSIONS OF THE CANADIAN BAR ASSOCIATION (BRITISH COLUMBIA BRANCH)

to the

LEGISLATIVE ASSEMBLY OF BRITISH COLUMBIA

SPECIAL COMMITTEE

TO REVIEW THE

PERSONAL INFORMATION PROTECTION ACT

Issued By:

Canadian Bar Association
British Columbia Branch

Special Committee of the
Freedom of Information and
Privacy Law Section

August 14, 2020

TABLE OF CONTENTS

PREFACE

Formed in 1896, the mission of the Canadian Bar Association (British Columbia Branch) (the "CBABC") is to:

- Improve the law;
- Improve the administration of justice;
- Improve and promote access to justice;
- Promote equality, diversity and inclusiveness in the legal profession and the justice system;
- Improve and promote the knowledge, skills, ethical standards and well-being of members of the legal profession;
- Provide opportunities for members to connect and contribute to the legal community;
- Represent the legal profession provincially, nationally and internationally; and
- Promote the interests of the members of The Canadian Bar Association.

The CBA nationally represents approximately 36,000 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.

The Freedom of Information and Privacy Law Section of the CBABC (the "Section") is pleased to respond to the call for submissions from the Legislative Assembly of British Columbia Special Committee ("Special Committee") to review the *Personal Information Protection Act,* R.S.B.C. 2003, c. 63 ("PIPA").[1]

The Section is comprised of members of the CBABC who share an interest, and/or practise law in areas that pertain to access of information and privacy law. As our membership represents a vast range of perspectives, interests and practices, it is difficult for the Section to make submissions to the Special Committee that would reflect the views of all members. Accordingly, rather than attempting to reconcile disparate points of view, the Section Executive decided to solicit and record input from individual members in its submissions to the Special Committee. As a result, the Section's submissions do not necessarily adopt a unified position on a particular issue. The following submissions reflect the views of individual Section members, and not necessarily the views of the CBABC or the Section as a whole.

This is the third occasion that a Special Committee has reviewed *PIPA*, and the third occasion that the Section has made submissions to the Special Committee.

[1] A copy of the legislation can be found at https://bit.ly/31KA2pZ.

The Section's 2014 Submissions

The Section's previous submissions dated September 14, 2014 (the "2014 Submissions") suggested changes to mandatory breach reporting, warrantless disclosure, constitutional considerations arising out of the Supreme Court of Canada's decision in *Alberta (Information and Privacy Commissioner) v. United Food and Commercial Workers, Local 401*, 2013 SCC 62, [2013] 3 SCR 733 ("*Alberta v. UFCW*")[2] and providing additional resources to the Office of the Information and Privacy Commissioner for British Columbia ("OIPC").[3]

The Special Committee's Report dated February 2015 adopted a number of the Section's suggested changes, including those related to warrantless disclosure.[4]

The Section's 2008 Submissions

The Section's previous submissions dated February 12, 2008 (the "2008 Submissions"), suggested changes regarding mandatory breach reporting, public interest discretion, settlement and confidential discussions, business transactions, cross-border data flows, and publicly available information.[5] The Special Committee's Report dated April 15, 2008 adopted a number of the Section's suggested changes, including those related to mandatory breach notification.[6]

---

[2] See https://bit.ly/2PK3K97.

[3] See https://bit.ly/2TsLl2P.

[4] See https://bit.ly/2TpbFuY, (the "Special Committee to Review the *Personal Information Protection Act* (2015)).

[5] See https://bit.ly/3kA9PmG.

[6] Streamlining British Columbia's Private Sector Privacy Law, https://bit.ly/2WOW21W.

EXECUTIVE SUMMARY

Section members submitted comments in relation to four issues. The first submission is about personal health information considerations as they relate to PIPA. Initiatives involving the proliferation of virtual medical care and those arising in the context of the COVID-19 pandemic, such as contact tracing apps and digital return to work apps, have highlighted the growing need in British Columbia ("BC") for health-specific privacy legislation. The second submission concerns the importance of maintaining consistency of PIPA with developments in national and international privacy legislation. While PIPA's existing framework is sound, PIPA has, in some respects, failed to keep pace with critical developments in Canadian and international privacy laws. The third submission is about the importance of protecting solicitor-client privilege. The Section recommends that amendments to PIPA are necessary to ensure there is no doubt about the protection afforded to the substantive right of solicitor-client privilege in PIPA. The final submission concerns the importance of amending PIPA to include mandatory privacy breach notification in order to increase the likelihood that PIPA will maintain its "substantially similar" status to the *Personal Information Protection and Electronic Documents Act,* S.C. 2000, c. 5 ("PIPEDA")[7], and to help protect British Columbians when they could suffer serious harm as a result of a privacy breach.

[7] See http://canlii.ca/t/541b8.

SUBMISSIONS

The Section members recommend changes in these areas:

1. Personal health information considerations, emergency measures and PIPA;
2. Importance of maintaining consistency with developments in national and international privacy legislation;
3. Protecting solicitor-client privilege; and
4. Mandatory privacy breach notification.

1. Personal health information considerations, emergency measures & PIPA

The Section would like to draw the Committee's attention to the unique circumstances to be considered when personal health information ("PHI") is collected, used and disclosed to deliver health services within the context of emerging technologies, like virtual health care apps, which bring together traditional and non-traditional health care providers in the public and private sectors. This submission considers the legislative landscape, potential inconsistencies in private and public sector privacy laws involving PHI, and compliance concerns in the context of a public health emergency.

Legislative Landscape: Privacy in a Public Health Emergency

On March 18, 2020, a state of emergency was declared for all of BC under the *Emergency Program Act* as a result of the COVID-19 pandemic. COVID-19 is unprecedented and it threatens the health and safety of people and government and business operations not only in BC but worldwide.

Government efforts in Canada to control the spread of COVID-19 have largely relied on manual and digital contact tracing and mandatory quarantine measures, which involve the collection, use and disclosure of personal information. Additional initiatives related to the proliferation of virtual care, COVID-19 contact tracing or exposure notification apps, and digital return to work apps, have highlighted the unique and sensitive nature of PHI. They have also highlighted the importance of placing strict limitations on the further use and disclosure of PHI collected by organizations, particularly in the context of a public health emergency.

The *Emergency Program Act* makes no mention of privacy, personal information or personal health information matters.[8] In 2020, the recent government consultation to modernize the *Emergency Program Act* in its Discussion Paper likewise did not mention privacy, personal information or personal health information.[9]

[8] See https://bit.ly/3cWkS5I.

[9] See https://bit.ly/3ioPgb8.

The *Public Health Act* (“PHA”) provides authority for and limits on the collection, use and disclosure of personal information by public health officials, including the disclosure by both public and private entities of personal information to those public health officials. Where the disclosure is not clearly permitted, the Provincial Health Officer is empowered to make any order necessary. However, what it does not squarely address, are the privacy implications that arise when public and private entities are then required to discharge certain public health surveillance functions.

The collection, use and disclosure of PHI is an issue that is relevant to both the public sector and the private sector, as well as to the interrelationship between them.

For example, as part of the BC Restart Plan, which supports the gradual re-opening and resumption of business operations, organizations have been specifically tasked with ensuring that their employees, customers, or patients who are ill or experiencing symptoms of COVID-19 are not permitted to be on the premises. This leaves private organizations grappling with how to operationalize this obligation, causing them to contemplate measures that may be privacy-invasive, such as temperature and wellness screening and digital contact tracing, with little guidance coming from public health officials or privacy regulators.

Even in situations where public health officials are able to provide meaningful parameters regarding the measures that are considered “necessary”, there is still

uncertainty regarding the types of limits on those measures that are considered to be "reasonable" in the context of PHI.

FIPPA vs. PIPA

Public bodies such as health authorities and hospitals are governed by the *Freedom Of Information And Protection Of Privacy Act*, R.S.B.C. 1996, c. 165 ("FIPPA").[10] FIPPA, while private-sector physicians, nurse practitioners, pharmacies, private laboratories and other allied health professionals in private practice (e.g. physiotherapists, dieticians, chiropractors, registered massage therapists, etc.) are governed by PIPA. Technology companies that create virtual health care apps, contact tracing apps, return to work apps etc. that involve the processing of PHI belonging to individuals in British Columbia are also subject to PIPA. The reality, however, is that all of these actors must work together and, in many cases, share PHI, in order to ensure an efficient and well-functioning health system.

This can prove to be difficult in practice, when the fundamental principles underpinning the privacy legislation that apply to public bodies on one hand, and private organizations on the other hand, are different. FIPPA is premised on a public body having a number of enumerated legal authorities to collect, use and disclose personal information, whereas PIPA is premised on individuals providing their consent. The result is that there are often obstacles to the necessary sharing of information and optimization of each player's role in the health system in circumstances where the public and private actors

[10] A copy of the legislation can be found at https://bit.ly/3iuHYCI.

in that system are increasingly being asked to collaborate to deliver a comprehensive and coordinated suite of health care services (e.g., the primary care networks).

Although both private healthcare providers and technology companies who innovate solutions involving PHI are governed by PIPA, the different industries they operate in can create a discrepancy in the privacy standards and controls that are implemented. For example, technology companies may not appreciate the sensitive nature of PHI, or understand their obligations regarding when it is appropriate to collect PHI, how to obtain valid consent, how to properly safeguard PHI, the limitations on secondary use and disclosure of PHI both within the workplace or to public bodies, and the deletion of PHI when the information is no longer required for the purposes for which the information was collected.

Health-Specific Privacy Legislation

These types of issues highlight the growing need in British Columbia for health-specific privacy legislation. Other provinces, like Alberta, Ontario, Manitoba, New Brunswick and others have legislation that considers the sensitive nature of PHI whether it is collected, used or disclosed by health providers in the private or public sector. This type of legislation can also create consistent standards for providers of health services, whether

the provider is a healthcare provider subject to regulation by their applicable College, or a private tech company launching a virtual health care app.

Section members invite the Special Committee to consider whether these types of concerns could be addressed by creating a more purpose-built health care-specific health information act for a "made in BC" solution. The Section's March 15, 2010 Submissions in response to the Special Committee's Third Legislative Review of FIPPA[11] encouraged the Special Committee to consider how other jurisdictions in Canada have created more fluid processes for health care-related information exchanges by enacting health-sector specific privacy legislation.

BC and Nunavut are the only jurisdictions in Canada that currently do not have health information management/privacy legislation. British Columbia has the *E-Health (Personal Health Information Access And Protection Of Privacy) Act*, but its scope and application is limited to certain designated health databases and does not address the concerns identified in this Submission. Other jurisdictions have managed to address some, but admittedly not all of these types of information sharing issues in their health information-specific legislation. For example, Alberta's *Health Information Act* has a limited definition of a "custodian", that may not extend to a private company that creates and operates a virtual care app, placing the responsibility to comply with the Act on physicians, nurses or other providers who meet the definition of a "custodian" but who

[11] See https://bit.ly/3ithKk3 at p.19.

may not have control in a meaningful way over the app or the continuity of care.[12] For British Columbia, this could be an opportunity to create tailored rights and obligations with respect to personal health information that will facilitate appropriate information sharing between all of the participants in the health sector, while also strictly limiting inappropriate sharing in recognition of the sensitivity of such information.

It must be noted that any proposed amendment or additional requirements to collect PHI during a public state of emergency should not be invoked to justify or legitimise collection of PHI during the course of ordinary business when the state of emergency has been lifted. This is to limit "scope creep" and the inappropriate and privacy-invasive secondary uses of PHI.

As the path to identifying the best solution for collection and sharing of PHI between the public and private sectors may require input that applies to PIPA, FIPPA and possibly new proposed legislation, the Section would be pleased to provide specific assistance as required by this Committee or in future consultations on this topic.

2. Importance of maintaining consistency with developments in national and international privacy legislation

British Columbia benefits from PIPA's consistency with provincial privacy laws, PIPEDA, and leading international privacy laws. Section members are of the view that the Legislature should follow and consider implementing important developments in privacy

[12] See section 1(1), https://bit.ly/3adIOAU.

law, in order to allow PIPA to provide democratic, social, and commercial advantages, as applicable to British Columbia. Strong privacy laws support other important and specific areas of law, including labour and employment, international trade, and consumer protection.

PIPA's existing framework is sound. It is a principles-based and technology neutral law. It is structured in a manner that allows organizations to evolve their privacy practices to reflect changing business models, technologies and customer expectations. It has proven to have some flexibility in adapting to rapidly evolving technologies (including the internet and "big data"), business practices and individual privacy expectations. Generally it works for all types and manners of organizations in respect of the personal information they collect, use, and disclose.

However, PIPA has, in some respects, failed to keep pace with developments in Canada and internationally. Other jurisdictions have been more agile in responding to changes in society and public expectations, legal developments and the application of new technology such as artificial intelligence or machine learning.

For example, PIPA does not establish some of the robust privacy rights that exist under the European Union (EU)'s *General Data Protection Regulation* ("GDPR")[13], which may be beneficial for British Columbians. As mentioned later in these Submissions, unlike PIPA, PIPEDA provides individuals with the right to be notified of privacy breaches

[13] See https://bit.ly/2FcvJfD.

where there is a real risk of significant harm. Organizations in British Columbia have fewer and less defined privacy obligations, and are subject to a weaker enforcement regime. In turn, this could not only affect PIPA's "substantially similar" status with PIPEDA, but could potentially impact Canada's "adequacy" status with European privacy laws.

PIPEDA

PIPA followed the passage of the federal privacy bill, PIPEDA, in 2001. Both British Columbia and Alberta adopted similar privacy laws that were deemed substantially similar to PIPEDA.

PIPA and PIPEDA are principles-based laws that reflect internationally-recognized fair information practices. PIPA should remain in line with other provincial privacy laws, and in particular, with PIPEDA, to facilitate consistent application of privacy laws across Canada. The Section recommends that the Legislature should follow additional changes to PIPEDA and consider whether amendments to PIPA are warranted to ensure PIPA is keeping pace for the benefit of British Columbians. Quebec's Bill 64 is an example of a province recognizing that its privacy laws are falling behind standards for best practices relating to privacy rights and protections, and enacting legislation that it believes meets the needs of individuals and organizations in Quebec.[14]

[14] See https://bit.ly/31FczH2.

GDPR

EU's privacy legislation, the GDPR came into force in May 2018. The GDPR has had a substantial and practical impact on organizations globally and in British Columbia. Privacy laws in non-EU jurisdictions, like Canada's PIPEDA, which are deemed to have protections that are "adequate" to European data protection laws, provide organizations in those non-EU countries commercial advantages by permitting the unrestricted transfer of personal information between Europe and the non-EU country. It is important and valuable from an economic and commercial perspective for Canada (and British Columbia, as a result of its "substantially similar" status to PIPEDA) to preserve the certainty and consistency in laws to help encourage cross-border data flows.

In the next year or so, the EU Commission will consider whether to maintain, repeal, amend or suspend Canada's adequacy status.[15] Part of this process involves looking more holistically at Canada's legal system and privacy regime as a whole, including privacy protections offered by provincial and territorial privacy and access to information laws, like PIPA. If PIPA fails to keep pace with PIPEDA and with foundational aspects of the GDPR, it could risk losing its "substantially similar" status to PIPEDA, as well as potentially negatively impact Canada's ability to maintain its adequacy status with the GDPR.[16]

[15] See https://ec.europa.eu/info/index_en.

[16] The Schrems 2 decision from the EU Court of Justice issued on July 16, 2020, provides a glimpse into the legal uncertainty created for organizations who transfer data from the EU into their own jurisdiction, when the adequacy status of that country's privacy legislation is repealed. This decision has left

The GDPR provides a good illustration for how PIPA could be modernized, as well as some of the challenges that can arise as a result of certain expanded privacy rights and protections. For example, Articles 12 to 22 of the GDPR expressly confer additional privacy rights to individuals that are not provided in PIPA. These include the right to erasure (right to be forgotten), the right to data mobility or data portability, and the right to restrict or object to data processing activities. The right to data portability is one area where implementation challenges have been identified since the GDPR has been in force, including the lack of standards enabling the provision of data in a machine-readable format.[17]

Another area relates to administrative fines. The GDPR provides data protection authorities with the ability to order administrative fines for non-compliance up to 20 million Euros or 4% of a company's global annual turnover. PIPA on the other hand provides courts with the power to order a fine up to $100,000 for an organization's non-compliance with PIPA. Changing PIPA's regime to one that mirrors the administrative fines in the GDPR would have significant consequences for organizations in British Columbia as well as on the OIPC's resources. Such impactful amendments, if contemplated, should include prior stakeholder consultations and careful consideration.

organizations that transfer EU personal data to the US scrambling to implement Standard Contractual Clauses and other measures to authorize the transfer. See https://bit.ly/2DYUfQE.

[17] See the European Commission's first evaluation report of the GDPR dated June 24, 2020, https://bit.ly/3kzhJwP.

Further, while PIPA primarily relies on consent (and a few narrow exceptions to consent) to authorize the collection, use and disclosure of personal information, Article 6 of the GDPR provides an organization with a number of other lawful authorities besides consent to facilitate processing, such as where the processing is necessary for:

- The performance of a contract to which an individual is a party or to take steps at the request of that individual prior to entering into a contract;
- Compliance with a legal obligation to which the controller is subject;
- Protecting the vital interests of an individual;
- The performance of a task carried out in the public interest; or
- The legitimate interests of the organization or a third party (except where those interests are overridden by the interests or fundamental rights and freedoms of the data subject).

While we do not see a compelling case for significant legislative change to the consent framework, we support the recognition that there are additional tools for facilitating lawful processing of personal information which should be permitted in circumstances where consent may not be practical. Consent has an important role to play in privacy protection and is achieved by the current PIPA framework, including in the context of accountability and other principles. Individuals should be empowered in decisions that impact their privacy rights, including maintaining their right to revoke consent.

However, in practice, meaningful consent is challenged by long and complex privacy terms or technological advancements like big data that have resulted in the collection,

use and disclosure of personal information in novel ways that were not necessarily contemplated when PIPA was enacted. Clearer requirements placed on organizations to be more transparent and accountable regarding their collection, use and disclosure of personal information, coupled with additional authorities (beyond consent) that permit the processing of personal information, may address some of these challenges.

Harmonization

Harmonizing rather than differentiating the application of these varied laws will improve data privacy knowledge of individuals and organizations in private and public sectors. Any changes to PIPA in light of changes to PIPEDA and the GDPR should carefully consider the resulting impact on BC organizations, and if there are preferable ways to enable continuing data flows to and from the EU without unduly restricting, in pursuit of the goal of adequacy, organizations' legitimate commercial activities occurring wholly within Canada.

The National CBA's recent submissions to Innovation, Science and Economic Development Canada's consultations included the following point on the topic of privacy law harmonization:[18]

[18] Canadian Bar Association Privacy and Access Law Section, "Strengthening Privacy for the Digital Age: Response to Proposals to Modernize PIPEDA" (December 2019), pp. 3-4, https://bit.ly/30LqPOY.

> Further harmonizing rather than differentiating the application of these varied laws will improve data privacy knowledge of individuals and organizations in private and public sectors. Any changes to PIPEDA in light of the GDPR should carefully consider the resulting impact on those same organizations, and if there are preferable ways to enable continuing data flows to and from the EU without unduly restricting, in pursuit of the goal of adequacy, organizations' legitimate commercial activities occurring wholly within Canada.
>
> ISED should conduct further analysis and consider potential issues with GDPR adequacy and monitor those developments carefully. If legal changes are required to maintain adequacy status, we believe that ISED should wait and see what specific changes will be called for and amend PIPEDA simultaneously to avoid confusion on the part of individuals and organizations.

If Parliament proposes changes to PIPEDA, Section members recommend that the Legislature explore whether specific related changes in PIPA are necessary to maintain consistency in practice as well as substantially similar status, and amend PIPA simultaneously to avoid potential confusion on the part of individuals and organizations.

Although the aforementioned considerations related to maintaining BC's substantially similar and Canada's adequacy status are important, the Section supports modernizing PIPA to include additional rights for individuals and organizations in a manner that makes sense within British Columbia's unique context. The Section cautions against a rushed approach of trying to fit novel privacy laws from other jurisdictions into British Columbia's existing privacy regime purely for the sake of harmonization. Before amendments to PIPA are introduced, it is important to consider the practical consequences and "lived experience" in the jurisdictions where these laws exist, to determine if they are appropriate for British Columbia.

If the Legislature moves forward with amendments, Section members suggest that consultations on reform be structured as widely as possible.

3. Protecting solicitor-client privilege

There has been much discussion over the last few years of the OIPC's power to compel production of documents that are protected by solicitor-client privilege under both public and private sector privacy and access legislation. While lawyers, the Law Society of British Columbia and others have sought to restrict or at least to temper the existing authority, the OIPC has, alone or with other commissioners across the country, argued that there is no risk to fundamental rights and sought greater authority and clearer statutory language to respond to judicial decisions that would restrict their power to compel information protected by the privilege.

PIPA exempts information that is protected by solicitor-client privilege from disclosure in response to a request for access to personal information.[19] PIPA also authorizes the Commissioner, for the purposes of conducting an investigation, audit or inquiry, to compel the production of documents "despite any privilege afforded by the law of evidence"[20] and provides that the solicitor-client privilege is not affected by the disclosure to the Commissioner.[21] In 2016, the Supreme Court of Canada decided a

[19] See s. 23(3)(a) of PIPA.

[20] See s. 38(5) of PIPA.

[21] See s. 38(3) of PIPA.

case called *Alberta (Information and Privacy Commissioner) v. University of Calgary*,[22] involving a challenge to similar language in the Alberta *Freedom of Information and Protection of Privacy Act.* At the heart of the case was whether section 56(3) of that Act, which required a public body to produce required records to the Commissioner "[d]espite . . . any privilege of the law of evidence", allowed the Alberta Commissioner and her delegates to review documents over which solicitor-client privilege was claimed. The Court concluded that solicitor-client privilege is not captured by the expression "privilege of the law of evidence"**,** that it cannot be set aside by inference but only by legislative language that is clear, explicit and unequivocal, and that the words "any privilege of the law of evidence" were insufficient to evince clear and unambiguous legislative intent to set aside solicitor-client privilege. This decision casts doubt on the extent to which the OIPC can compel the production of documents protected by solicitor-client privilege and the issue is currently being litigated in the BC Supreme Court. This portion of our Submission addresses our Section's concerns about the impact of the OIPC's power to compel production of documents, and the way in which it has recently been exercised.

[22] See 2016 SCC 53, [2016] 2 S.C.R. 555, https://bit.ly/30L7f5v.

The Importance of Solicitor-Client Privilege

Once merely a privilege of the law of evidence which protected litigants from being compelled to testify, solicitor-client privilege has been recognized as more than an evidentiary rule since 1979.[23] By 1982 solicitor-client privilege was determined to be a substantive right, formulated as follows.[24]

1. The confidentiality of communications between solicitor and client may be raised in any circumstances where such communications are likely to be disclosed without the client's consent.

2. Unless the law provides otherwise, when and to the extent that the legitimate exercise of a right would interfere with another person's right to have his communications with his lawyer kept confidential, the resulting conflict should be resolved in favour of protecting the confidentiality.

3. When the law gives someone the authority to do something which, in the circumstances of the case, might interfere with that confidentiality, the decision to do so and the choice of means of exercising that authority should be determined with a view to not interfering with it except to the extent absolutely necessary in order to achieve the ends sought by the enabling legislation.

4. Acts providing otherwise in situations under paragraph 2 and enabling legislation referred to in paragraph 3 must be interpreted restrictively.

Over the ensuing almost forty years, the essential importance of solicitor-client privilege to a well-functioning justice system became clearer. By 2016, in the *University of*

[23] *Solosky v. The Queen*, 1979 CanLII 9 (SCC), https://bit.ly/2PJj6e3.

[24] *Descôteaux v. Mierzwinski*, 1982 CanLII 22 (SCC), [1982] 1 SCR 860, https://bit.ly/33W9XHz.

Calgary case, Justice Côté of the Supreme Court of Canada concluded that the importance of solicitor-client privilege to our justice system "can't be overstated"[25] because it is concerned with the protection of a relationship that has a central importance to the legal system as a whole. Communications between solicitor and client are essential to the effective operation of the legal system. The right protects and facilitates access to justice by enabling frank, open and completely confidential disclosure by clients to their lawyers of all information relevant to their legal problem. Our legal system is premised on the notion of equally matched parties, both represented by knowledgeable advocates who can advise their clients about the legal implications of their situation, and who zealously advance their client's case before an impartial adjudicator. The privilege exists to ensure that the client can trust that what she tells her lawyer will be protected from further disclosure. This trust promotes full disclosure by the client and ensures that the lawyer understands all relevant facts, which is necessary to assess her potential legal jeopardy and provide relevant advice. The lawyer must know "the good, the bad and the ugly" in order to advise the client about the appropriateness of defending, settling or making other decisions within the litigation process. The absence of confidentiality undermines the ability of the lawyer to represent the client, thus impairing the right to a fair adjudicative process, and denying the client access to justice. For these reasons, solicitor-client privilege has been recognized as cornerstone of our legal system and has acquired constitutional

[25] *Alberta (Information and Privacy Commissioner) v. University of Calgary*, *supra* at para. 26.

dimensions as both a principle of fundamental justice and as part of a client's fundamental right to privacy.[26]

This is why solicitor-client privilege belongs to the client, not to the lawyer. No solicitor has the right to disclose a client's information without the consent of the client because solicitor-client privilege is the individual's fundamental right, inexorably linked to the individual's constitutional rights.

Furthermore, we submit that solicitor-client privilege is a principle of fundamental justice because if a citizen can't trust their lawyer to keep their confidences, she can't trust the system to be fair or independent. Trust in the fairness and independence of the legal system is of paramount concern in a democracy. At its core, solicitor-client privilege exists to protect everyone from the damage to the democratic legal system that can be done when fundamental rights are infringed in the guise of investigatory efficiency. The Court in the *University of Calgary*[27] decision said that:

> It is indisputable that solicitor-client privilege is fundamental to the proper functioning of our legal system and a cornerstone of access to justice (Blood Tribe, at para. 9). Lawyers have the unique role of providing advice to clients within a complex legal system (McClure, at para. 2). 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 (see Smith v. Jones, 1999 CanLII 674 (SCC), [1999] 1 S.C.R. 455, at para. 46). It is therefore in the public interest to protect solicitor-client privilege. For this

---

[26] *Alberta (Information and Privacy Commissioner) v. University of Calgary*, *supra*, at para. 20; *R. v. McClure*, 2001 SCC 14, [2001] 1 S.C.R. 445, at para. 4, https://bit.ly/31GgMtX; *Lavallee, Rackel & Heintz v. Canada (Attorney General)*, 2002 SCC 61, [2002] 3 S.C.R. 209, at para. 46, https://bit.ly/30KeWJg. See also *Canada (National Revenue) v. Thompson*, 2016 SCC 21, [2016] 1 S.C.R. 381, at para. 17, http://canlii.ca/t/grxb3.

[27] *Alberta (Information and Privacy Commissioner) v. University of Calgary*, *supra* at paras. 26, 34.

> reason, “privilege is jealously guarded and should only be set aside in the most unusual circumstances” (Pritchard, at para. 17).

Following a long line of cases dating back to 1979, the Supreme Court in the *University of Calgary* case held that to give effect to solicitor-client privilege as a fundamental policy of the law, legislative language purporting to abrogate it, set it aside or infringe it must be interpreted restrictively and must demonstrate a clear and unambiguous legislative intent to do so.

In the aftermath of the *University of Calgary* decision, Canada’s federal, provincial and territorial Information and Privacy Commissioners issued a joint resolution in 2017 calling for amendments to access to information and privacy legislation to express the unambiguous intention that the associated Commissioner is authorized to compel the production of records over which solicitor-client privilege is claimed in order to determine whether this exemption has been properly asserted.[28] In this resolution, the Commissioners’ recitals stated, in part:

- Canada’s IPCs recognize the importance of the protections afforded by solicitor-client privilege for the proper functioning of Canada’s legal system;
- The IPCs have practices and procedures in place to ensure confidentiality and security of information provided to them, including information over which public bodies have claimed solicitor-client privilege;
- Providing IPCs with records over which solicitor-client privilege is claimed for the purposes of independent review does not constitute waiver of this privilege. The IPCs’ review of these records is only to confirm whether they

[28] See Safeguarding Independent Review Of Solicitor-Client Privilege Claims: Resolution of the Federal, Provincial and Territorial Information and Privacy Commissioners (October 17-18, 2017), https://bit.ly/2XQTpfU.

> are subject to solicitor-client privilege. IPCs do not disclose the records or use them for any other purpose.

The Commissioners argue that their independent review function "fundamentally depends on their ability to examine responsive records over which public bodies claim exemptions, including the exemption for solicitor-client privilege, in order to determine that such claims have been properly asserted." This position is also reflected in the OIPC's 2016 submission to the Special Committee to Review the *Freedom of Information and Protection of Privacy Act* in respect of the authority under that Act to compel records subject to solicitor-client privilege for the purposes of an investigation, audit or inquiry. The OIPC submitted that this authority does not threaten any fundamental rights because the records "are not made public or put to any purpose other than verifying that the exemption to the right of access has been properly applied" and that "[t]here is no risk of the records being disclosed until all avenues of appeal are exhausted, and then disclosure is made by the public body, not by the Commissioner."[29]

Recent developments have raised questions about these assertions and the OIPC's authority. In November 2019, LifeLabs, a lab-testing company advised the OIPC that it had a privacy breach as a result of a cyberattack on its computer systems.[30] The OIPC investigated. On February 7, 2020, the Commissioner exercised his authority under section 38(1)(b) of *PIPA*, to order LifeLabs to produce its audit report on the

[29] See at p. 19, https://bit.ly/33QXwfO.

[30] See "LifeLabs Privacy Breach: FAQs" (December 17, 2019), https://bit.ly/33T9e9Q.

cyberattack. Section 38(5) of PIPA further provides that a copy of any document required by the Commissioner under section 38 must be provided to the Commissioner "despite any privilege afforded by the law of evidence." LifeLabs claimed solicitor-client privilege and litigation privilege over its audit report and refused to comply with the Commissioner's order on the basis that section 38(1)(b) does not allow the Commissioner to compel production of documents protected by solicitor-client privilege and litigation privilege. On February 20, 2020, LifeLabs filed a petition in BC Supreme Court for a declaration that the Commissioner cannot compel production of LifeLabs' audit report under section 38(1)(b) of *PIPA*. To date, the matter is still before the BC Supreme Court.

On June 25, 2020, the BC OIPC and the Ontario IPC issued a joint news release announcing the conclusion of their joint investigation and their finding that LifeLabs had failed to implement reasonable safeguards in violation of Ontario's *Personal Health Information Protection Act* and BC's PIPA. In their joint statement, the Commissioners said that the publication of their report was "being held up by LifeLabs' claims that information it provided to the commissioners is privileged or otherwise confidential.[31] The Commissioners reject these claims. The IPC and BC OIPC intend to publish the report publicly unless LifeLabs takes court action." Subsequently on July 29 they issued a second release, stating:

> Commissioners Patricia Kosseim (Ontario) and Michael McEvoy (B.C.) maintain the view that the public release of the joint investigative report is vital to bringing to light the underlying causes of the privacy breach and rebuilding public trust by providing a transparent account of their investigation and findings. However,

[31] See https://bit.ly/3afiSEQ.

> LifeLabs has decided to seek a court order preventing the public release of the commissioners' joint investigation report claiming that some of the information it provided to the commissioners is privileged or otherwise confidential, a claim which the commissioners take issue with. As this matter is now before the courts, our offices will not be providing any further comment at this time.[32]

The Section submits that this position is inconsistent with what the OIPC said in 2016, and what all the Commissioners in Canada said in 2017, would never happen. Specifically, a client's privileged information provided to the Commissioners pursuant to their power of compulsion in the course of an investigation, is now at risk of being disclosed in a public report against the wishes or intentions of the client.

The Commissioners are taking an adversarial position in this issue. The language in the press release implies that efforts by LifeLabs to protect privileged and confidential information is an attempt to delay the Commissioners' legitimate exercise of their authority.

The Supreme Court in the *University of Calgary* decision presaged this problem when it said that that compelled disclosure to the Commissioner for the purpose of verifying solicitor-client privilege is itself an infringement of the privilege, regardless of whether or not the Commissioner may disclose the information onward to the applicant, but noted that the Commissioner is not an impartial adjudicator of the same nature as a court. The Commissioner may exercise both adjudicative and investigatory functions and can become adverse in interest to a public body (or an organization). The Commissioner

[32] See https://www.oipc.bc.ca/news-releases/3449.

may take the organization to court if it refuses to disclose information and become a party in litigation against that organization.[33] This observation was merely theoretical in 2016 but the LifeLabs dispute illustrates how disclosure to the OIPC is an infringement of the privilege that can lead to a potentially serious incursion on substantive, fundamental rights.

The Rules of Court are less invasive

The Section agrees that there is a responsibility to provide the OIPC with sufficient information to support a claim for privilege. However, an order to release solicitor-client privileged information to the OIPC goes far beyond what even a judge would order in court.

For example, the B.C. Rules of Civil procedure provide the following:

[33] *Alberta (Information and Privacy Commissioner) v. University of Calgary*, *supra* at paras. 35-36.

Rule 7-1 — Discovery and Inspection of Documents

Claim for privilege
(6) If it is claimed that a document is privileged from production, the claim must be made in the list of documents with a statement of the grounds of the privilege.

Nature of privileged documents to be described
(7) The nature of any document for which privilege from production is claimed must be described in a manner that, without revealing information that is privileged, will enable other parties to assess the validity of the claim of privilege.[34]

In general circumstances, a judge would not require a party asserting a claim of privilege to produce the document itself. Rather, the party is only required to provide sufficient information for the other side to assess the privilege claim, without revealing privileged information. A judge would not order a privileged document to be produced except in very limited circumstances. In contrast, the Commissioners claim entitlement to order disclosure of privileged information for their review and inspection, while retaining the authority to impose sanctions on the party releasing the document. This approach is fundamentally at odds with principles of fundamental justice.

As the process under the Rules of Court amply demonstrate, any claim of solicitor-client privilege can adequately be addressed by providing the Commissioner with enough information to assess the claim for privilege, without revealing the privileged information itself.

[34] See https://bit.ly/2PIbtV4.

Solicitor-Client Privilege & the Federal Privacy Act

Recently, Canada enacted *An Act to Amend the Access to Information Act and the Privacy Act and to make consequential amendments to other Acts* (Bill C-58, Chapter 18, 2019) ("Bill C-58").[35] Bill C-58 made amendments to the *Access to Information Act* and the *Privacy Act* to permit the Canadian Information and Privacy Commissioners, respectively, to review records withheld by the head of a government institution on the basis that they are protected by solicitor-client privilege, professional secrecy or litigation privilege. Specifically, section 15 of Bill C-58 amends the *Access to Information Act* and section 50 of Bill C-58 amends the *Privacy Act*; these 2 provisions have parallel wording; these 2 provisions are not yet in force, but come into force by future regulation.

The national CBA made submissions to the Canadian Parliament on Bill C-58 recommending that sections 15 and 50 be removed from Bill C-58 in order to protect solicitor-client privilege.[36] In those submissions, the national CBA highlighted the purpose and importance of solicitor-client privilege as articulated by the Supreme Court (see above).

[35] See https://bit.ly/3ahs37O.

[36] See https://bit.ly/3g8n3VP ("CBA's Bill C-58 Submissions").

The national CBA identified the following concerns with section 15 and 50 of Bill C-58:

> There are important practical consequences to these proposed amendments.
>
> Today, legal advice is developed as part of a dynamic exchange between lawyer and client, and the advice given provides calculations of risk reflecting the complex, strategic considerations appropriate to the public sector context. It is essential that clients feel comfortable exploring a wide range of scenarios with their legal advisors, to be fully informed of the legal dimensions of their decisions. If they cannot be confident about the protections of solicitor-client privilege, there will invariably be a chilling effect in seeking frank legal advice, to the detriment of the proper functioning of government.
>
> **Who should adjudicate solicitor-client privilege disputes?**
>
> The prudent course in this context is to ensure that assessments of disputed privilege claims are made by the judiciary. If the heads of government institutions follow best practices for discovery of privileged records, these disputes should be rare and constitute an appropriate use of judicial resources.
>
> There is no requirement that the person who holds the office of Information or Privacy Commissioner have particular expertise on solicitor-client privilege. Further, unlike the courts, the Commissioners are not impartial adjudicators. Bill C-58 would authorize the Information Commissioner to appear in court on behalf of a complainant or in their own right as a party. As such, the Commissioner can become adverse in interest to a public body. Similar powers are accorded the Privacy Commissioner.
>
> Compelled disclosure of the federal government's privileged information to the Information or Privacy Commissioner, even for the limited purpose of verifying the privilege claim, is a serious intrusion on the privilege. Compelled disclosure to a potential adversary is all the more serious.[37]

[37] CBA's Bill C-58 Submissions at pp. 30-31.

Solicitor-Client Privilege and PIPA

Since coming into force in 2004, *PIPA* has recognized and protected solicitor-client privilege. Section 3(3) of *PIPA* provides that "nothing in this Act affects solicitor-client privilege."

In both the 2008 and 2014 review of *PIPA*, the Law Society of BC tendered evidence before the Special Committee to recommend that *PIPA* be amended to further protect solicitor-client privilege on this basis:

> Section 38(5) of PIPA provides that a copy of any document required by the Commissioner under section 38 must be provided to the Commissioner "despite any privilege afforded by the law of evidence." The Committee received evidence from the Law Society of British Columbia that this provision is inconsistent with section 3(3) of PIPA, which provides that "nothing in this Act affects solicitor-client privilege." The Law Society submitted that the power of the Information and Privacy Commissioner to compel the production of a document despite solicitor-client privilege should be removed because it does not adequately and properly protect the public interest in the administration of justice. If a question of privilege is being raised in connection with a document, the matter should be dealt with by the Supreme Court.[38]

The 2015 Special Committee's report considered the Law Society's evidence but declined to recommend that the change be made.

Bill C-58 has shifted the debate across Canada as to whether an information or privacy commissioner can, or should, have authority to review withheld records for the purpose of verifying a claim of solicitor-client privilege by the head of a public body. The Section

[38] Special Committee to Review the *Personal Information Protection Act* (2015) at pp. 24-25, https://bit.ly/3iBeinz.

is very concerned that as a result, in other jurisdictions across Canada, the pendulum has shifted toward weakening solicitor-client privilege in this context. The Section submits that review of solicitor-client privilege claims should remain with the judiciary.

The Section understands that the Special Committee is concerned with the question of efficiency because of the delay and cost a requestor may experience by participating in the court process to dispute a privilege claim. The Section submits that requiring an applicant to participate in the court process if the applicant continues to dispute a solicitor-client privilege claim after the OIPC Request for Review process is complete does not result in any material loss of the applicant's rights to the same extent that requiring a party to release solicitor-client privileged material necessarily would. Further, the risk of delay and cost should not override a fundamental right. As a practical matter, disputes about solicitor-client privileged records are likely to end up in court in any event due to their complexity, and the organization or public body will be the one required to defend its position before the courts, as seen in the LifeLabs case.

The Section submits that, in practice, there are likely a limited number of these types of cases. A review of the case law shows that the OIPC's orders or decisions in respect of solicitor-client privilege have been overturned on judicial review a sufficient number of times to suggest that it is important for these types of claims to remain with the judiciary.

The Section has considered alternate approaches, and is of the view that even if the Special Committee were to recommend a parallel administrative process for review of

solicitor-client privilege claims, that process would still result in delay while the claim is being adjudicated.

One has only to look to the delay inherent in other administrative tribunal proceedings, like the Human Rights Tribunal ("Tribunal"). While administrative bodies make best efforts to operate as efficiently as possible, the process of adjudicating a dispute necessarily takes some time. We note that the Tribunal, like a judge, would not order disclosure of information protected by solicitor-client privilege in order to assess the privilege claim except in the most egregious circumstances; the Tribunal would simply ask for enough information to assess the claim of privilege.

The Section submits that rather than abrogating a right as fundamental as solicitor-client privilege, more active education of unsophisticated parties would be a more appropriate approach. As above, the Section is also supportive of providing sufficient information to the OIPC to support the solicitor-client privilege claim, similar to the provisions found in the Rules of Court. Any remaining disputes should remain with an independent adjudicator like the judiciary.

Conclusion on solicitor-client privilege

These concerns raised by the CBA by Bill C-58 and as a result of the LifeLabs case are equally applicable to empowering the OIPC through *PIPA* amendments or court orders to be able to encroach on solicitor-client privilege.

Concerns about an organization improperly applying the solicitor-client privilege exemption cannot be addressed internally by the OIPC because verifying the application of solicitor-client privilege requires a legal determination by an impartial decision maker. The Section therefore supports the Law Society's 2008 and 2014 requests to amend section 38 of *PIPA* to ensure solicitor-client privilege is protected.

As a result, and in view of the Supreme Court's decision in *University of Calgary,* Section members recommend that the Special Committee ensure that there is no doubt about the protection afforded the substantive right of solicitor-client privilege in PIPA by:

i. Amending section 38(5) of PIPA to clarify that the OIPC power to compel production of records under that subsection does not extend to documents protected by solicitor-client privilege; and

ii. Amending PIPA to add a provision prohibiting the Commissioner from publicly disclosing information obtained by it in the course of an investigation, audit or inquiry, where a party asserts solicitor-client privilege over such information, unless that party expressly consents to the disclosure.

4. Mandatory Privacy Breach Notification

The Section's February 12, 2008 Submissions

In its 2008 Submissions to the Special Committee, the Section advanced the varying views of its members with respect to the issue of mandatory breach notification. While members' views varied regarding the necessity of introducing a mandatory requirement, there was general consensus that if such a requirement were to be introduced, careful consideration would need to be given to the following:

- **Threshold requirements** – articulating a clear threshold requirement for reporting to the OIPC, for example, the number of individuals affected, categories of information lost, recipient of the notification and timelines for and methods of effecting notification; and
- **Consistency** – ensuring that the substance of the threshold requirements is essentially the same under PIPA, PIPEDA and the Alberta *Personal Information Protection Act* ("Alberta PIPA*"*).

The Special Committee recommended in its April 2008 report that PIPA should include a provision expressly requiring organizations to notify affected individuals of certain privacy breaches related to unauthorized disclosure and use of sensitive financial or health information.[39] To date, the Special Committee's recommendation has not been implemented.

[39] Streamlining British Columbia's Private Sector Privacy Law, *supra* at pp. 7-8.

The Section's 2014 Submissions

In its 2014 Submissions to the Special Committee, the Section reviewed the introduction of mandatory breach notification under the Alberta PIPA, as well as the then-upcoming amendments to PIPEDA, both of which are discussed further below.

The Section also discussed the June 2014 submissions of the CBA at the National level to the Standing Senate Committee on Transport and Communications on the then-upcoming amendments to PIPEDA. Among other things, the National CBA drew this Committee's attention to the need and desire to avoid the U.S. experience with breach notification, where a multitude of approaches adopted in various state and federal laws have created and imposed on organizations a confusing, inconsistent patchwork of obligations.

Since the Section's 2014 submissions, privacy laws in other provinces, federally, and internationally have been amended to include mandatory breach reporting provisions.

Mandatory Privacy Breach Reporting in Other Jurisdictions

When it comes to mandatory privacy breach reporting, PIPA has fallen behind other provincial, federal and international privacy laws. Most recently, Quebec's Bill 64 includes an obligation for enterprises to notify the Quebec privacy regulator of "confidentiality incidents" that present a "risk of serious harm", and imposes high administrative penalties for non-compliance of up to up to $10 million or 2% of

worldwide turnover and penal sanctions of up to $25 million or 4% of worldwide turnover (whichever is greater). Many jurisdictions in Canada have specific health sector privacy legislation that requires breach reporting to the relevant professional and/or privacy regulators. If Quebec's Bill 64 passes, BC will be the only province left in Canada that has no mandatory privacy breach reporting whatsoever in any health sector, public sector, or private sector privacy legislation.

This gap is putting the safety of British Columbians at risk because they have no legal right to be informed when their personal information is part of a privacy breach, regardless of whether or not they could suffer serious harm as a result. Alberta's approach in PIPA and the Federal Government's approach in PIPEDA could serve as an example for how BC might create a mandatory breach notification regime within PIPA that has similar thresholds and processes and facilitates a consistent approach to mandatory privacy breach reporting.

Alberta

In 2009, following the recommendations of its own Special Committee, Alberta amended the Alberta PIPA to include a mandatory breach notification requirement.

- **Reporting threshold –** section 34.1 of the Alberta PIPA requires an organization to provide notice, without unreasonable delay, to the Alberta Information and Privacy Commissioner (the "Alberta OIPC") of any incident involving the loss of, unauthorized access to, or unauthorized disclosure of personal information that

was under the organization's control where a reasonable person would consider that the exists a real risk of significant harm to an individual as a result of the loss or unauthorized access or disclosure. The notice to the Alberta OIPC must conform to requirements set out in section 19 of the Personal Information Protection Act Regulation (the "Alberta PIPA Regulation").[40]

- **Notification to affected individuals** – section 37.1 of the Alberta PIPA, provides that the Alberta OIPC may require a reporting organization to notify individuals to whom there is a real risk of significant harm as a result of the loss or unauthorized access or disclosure, in accordance with the information requirements set out in section 19.1 of the Alberta PIPA Regulation, and within the timeline imposed by the Alberta OIPC. In practice, organizations often notify both the Alberta OIPC and affected individuals at the same time out of prudence. The Alberta OIPC can also impose additional terms and conditions on the organization in connection with the notification as the Alberta OIPC deems appropriate, as provided in section 37.1(2) of the Alberta PIPA.

- **Voluntary notification** – section 37.1(7) provides that nothing in the mandatory breach notification requirement prevents an organization from notifying individuals voluntarily.

[40] See Alta. Reg. 366/2003, https://bit.ly/3kAB9RM.

- **Failure to notify is an offence** – section 59(1)(e.1) provides that it is an offence under the Alberta PIPA to fail to notify the Alberta OIPC when required by section 34.1. The penalty for committing an offence is a fine of not more than $10,000 for individuals, or $100,000 for persons other than individuals. Pursuant to section 59(4), neither an organization nor an individual may be found guilty of an offence if they can demonstrate to the satisfaction of the court that they active reasonably in the circumstances that gave rise to the offence.

Canada (Federal)

On November 1, 2018, amendments to PIPEDA came into force, establishing mandatory breach notification federally.

- **Reporting threshold** – organizations must notify the Privacy Commissioner of Canada if there is a "breach of security safeguards involving personal information under an organization's" control if it is reasonable in the circumstances to believe that the breach creates a real risk of significant harm to an individual".[41] Significant harm is defined in section 10.1(7) as including "bodily harm, humiliation, damage to reputation or relationships, loss of employment, business or professional opportunities, financial loss, identity theft, negative effects on the credit record and damage to or loss of property." Section 10.1(8) provides that, in determining whether a breach creates a real risk of significant harm, an

[41] Sections 10.1(1) and (3).

organization must consider the sensitivity of the personal information involved in the breach and the probability that it is or will be misused.

- **Notification to affected individuals and third parties** - If the regulator notification threshold is reached, the organization must also notify affected individuals. The report and notice must be made as soon as feasible, and must comply with the requirements of sections 2-5 of the Breach of Security Safeguards Regulations under PIPEDA.[42] Pursuant to sections 10.2(1) and (2), the organization that suffers the breach must also notify other organizations or government institutions of the breach as soon as feasible if the notifying organization believes that the other organization or the government institution or part concerned may be able to reduce the risk of harm that could result from it or mitigate that harm.

- **Breach log** - Further, section 10.3 requires the organization to maintain a breach log of every incident where there has been a breach of security safeguards, even when the real risk of harm threshold has not been met. PIPEDA makes it an offence if an organization fails to notify the Privacy Commissioner of Canada, fails to notify affected individuals and fails to keep a breach log where required, subject to a court-ordered fine not exceeding $100,000.

[42] SOR/2018-64, https://bit.ly/2Fgd5DL.

Europe

Articles 33 and 34 of the GDPR require information controllers (which includes both private organizations and public bodies) to both report privacy breaches to the regulatory authority with jurisdiction over them, as well as notify affected individuals. Reports to the regulatory authority are required unless the breach "is unlikely to result in a risk to the rights and freedoms of natural persons". Notice must be given to affected individuals where the breach "is likely to result in a high risk to the rights and freedoms of natural persons". Articles 33 and 34 also specify the content of the report and notice.

The report and notice must be completed "without undue delay". If the report to the regulatory authority is not completed within 72 hours of the controller becoming aware of it, the report must include the reason for the delay. Failure to report and notify can result in substantial administrative fines outlined earlier in our submissions.

Current Submissions

In the Section's 2014 submissions, prior to the enactment of the PIPEDA amendments, the Section stated that "given the legislative activity elsewhere in Canada, there is a sense of inevitability that [mandatory breach reporting] will be introduced in British Columbia."[43]

[43] Page 18.

The entry into force of the GDPR mandatory breach reporting scheme further underscores this inevitability on an international level. The Section's previous concerns about PIPA's continued designation as "substantially similar" to PIPEDA, as well as Canada's ability to maintain its adequacy status with EU privacy laws, also persist. As stated in the Regulatory Impact Analysis Statement released by the Privacy Commissioner of Canada, PIPEDA was amended to include mandatory breach reporting in part to harmonize with the GDPR given that many Canadian organizations must comply with both Canadian and European law.[44]

Further, ensuring that PIPA keeps harmony and consistency with mandatory privacy breach reporting regimes in other provinces, PIPEDA and the GDPR, in terms of the thresholds and processes required for mandatory breach reporting, can result in commercial benefits to British Columbia by facilitating the unimpeded flow of personal information to and from other jurisdictions, and guarantee a strong standard of protection for personal information in both jurisdictions. The Section urges the Special committee, in contemplating and recommending reporting and notification thresholds and processes, to take into account the following considerations:

- Giving the OIPC the ability to order organization to notify affected individuals and the powers to enforce those orders;

[44] See Regulatory Impact Analysis Statement for Breach of Security Safeguards Regulations: SOR/2018-64 (Office of the Privacy Commissioner of Canada), (2018) C Gaz II, 703 (*Personal Information Protection and Electronic Documents Act)*, https://bit.ly/2DXJf65.

- Limiting mandatory breach reporting to material incidents, such as those that that raise a “real risk of significant harm” to individuals;
- Having a single threshold for reporting to the OIPC and to affected individuals, as seen under PIPEDA, the Alberta PIPA and the GDPR;
- Imposing a flexible and realistic approach to how quickly organizations must report;
- Requiring organizations who experience a “reportable breach incident” to take corrective action;
- Determining whether noncompliance with mandatory reporting obligations should result in meaningful financial consequences to organizations or be addressed under the current complaints process; and
- Assisting the OIPC to more accurately track the number, magnitude and type of breaches, which are currently being reported to the OIPC on an *ad hoc* or voluntary basis.

Section members agree that the Special Committee should deliberate on the role that mandatory breach reporting may serve, and ensure that BC’s privacy breach reporting regime, if enacted, is consistent to the extent reasonably possible with other breach notification regimes in Canada and abroad.

SUMMARY OF RECOMMENDATIONS TO THE SPECIAL COMMITTEE

The Section recommends that:

1. The Special Committee consider whether concerns specific to personal health information are best addressed by creating a purpose-built health care-specific health information act.
2. The Special Committee consider amendments to PIPA based on developments in the GDPR and future developments in PIPEDA to help maintain PIPA's "substantially similar" status to PIPEDA as well as Canada's "adequacy" status to EU privacy laws, to the extent that they make sense within the BC context, and that prior consultations on reform be structured as widely as possible.
3. The Special Committee clarify and strengthen the protection afforded by the substantive right of solicitor-client privilege in PIPA by:
    a. amending section 38(5) of PIPA to clarify that the OIPC power to compel production of records under that subsection does not extend to documents protected by solicitor-client privilege; and
    b. amending PIPA to add a provision prohibiting the Commissioner from publicly disclosing information obtained by it in the course of an investigation, audit or inquiry, where a party asserts solicitor-client privilege over such information, unless that party expressly consents to the disclosure.
4. The Special Committee amend PIPA to include mandatory privacy breach notification, and ensure that any such regime is consistent, to the extent reasonably possible, with other breach notification regimes in Canada and internationally.

CONCLUSION

We would be pleased to discuss our submissions further with the Special Committee in person, by virtual means, or in writing, in order to provide any clarification or additional information that may be of assistance to the Special Committee.

Communications in this regard can be directed to:

SINZIANA GUTIU
Co-Chair, CBABC Freedom of Information and Privacy Law Section
Tel.: (778) 689-2537
Email: sinziana.gutiu@telus.com

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