THE CANADIAN BAR ASSOCIATION
L'ASSOCIATION DU BARREAU CANADIEN
INFLUENCE. LEADERSHIP. PROTECTION.

CCCA ACCJE 25 Years of In-House Excellence
Ans d'excellence en conseil juridique d'entreprise

Bill S-4 – *Digital Privacy Act*

CANADIAN BAR ASSOCIATION

June 2014

500-865 Carling Avenue, Ottawa, ON, Canada K1S 5S8
tel/tél : 613.237.2925 | **toll free/sans frais** : 1.800.267.8860 | **fax/téléc :** 613.237.0185 | **info@cba.org** | **www.cba.org**

PREFACE

The Canadian Bar Association is a national association representing 37,500 jurists, including lawyers, notaries, law teachers and students across Canada. The Association's primary objectives include improvement in the law and in the administration of justice.

This submission was prepared by the CBA's Privacy and Access Law Section and Canadian Corporate Counsel Association, with the input of the Elder Law Section. The submission has been reviewed by the Legislation and Law Reform Committee and is approved as a public statement of the Canadian Bar Association.

TABLE OF CONTENTS

Bill S-4 – *Digital Privacy Act*

Bill S-4 – *Digital Privacy Act*

I. INTRODUCTION

The Canadian Bar Association's Privacy and Access Law Section and Canadian Corporate Counsel Association (collectively, the CBA) welcome the opportunity to comment on Bill S-4, the *Digital Privacy Act*, which proposes amendments to the *Personal Information Protection and Electronic Documents Act* (PIPEDA). The CBA Elder Law Section also contributed on the issue of disclosure without consent in the context of suspected financial abuse.

The Privacy and Access Law Section comprises lawyers with in-depth knowledge in the areas of privacy and access to information. The Section is active in commenting on developments in privacy and access to information law and policy, and has participated in numerous submissions to government on the various iterations and reviews of PIPEDA.

The Canadian Corporate Counsel Association (CCCA) is the national forum for in-house counsel, including lawyers practicing in corporations, business enterprises, associations, institutions, not-for-profit organizations, government and regulatory board and agencies, Crown corporations, and regional or municipal corporations. The CCCA has frequently commented on draft legislation and government consultations related to their members' area of practice, including the appropriate balance between the facilitation of commerce and individual privacy rights.

The CBA recognizes that governments and organizations have legitimate reasons to collect, use and disclose personal information for limited purposes. We encourage vigilance in monitoring and opposing unnecessary erosions of privacy, and support the principle that collection, use and disclosure of personal information without knowledge and consent be conducted in a manner that is reasonable and necessary in the circumstances. [1] Our comments and recommendations on Bill S-4 are from that perspective.

---

1 www.cba.org/CBA/resolutions/pdf/04-05-A.pdf

II. SUMMARY OF RECOMMENDATIONS

The CBA supports the objectives of Bill S-4. The proposed amendments to PIPEDA are aligned in many respects with past CBA recommendations for improvements to the legislation. We agree with the inclusion of new provisions on disclosure of personal information in the course of business transactions and on breach notification, and support the replacement of the investigative body paradigm with a model of reciprocal collection, use and disclosure exemptions. We offer a number of suggestions for improvement, particularly to ensure that the scope of the permitted disclosure, and the steps to be taken before and after disclosure, are appropriate.

Both Bill S-4 and Bill C-13, the *Protecting Canadians from Online Crime Act,* address privacy rights in the digital age. Although there are clear distinctions between their scope and application, both establish rules for the non-consensual disclosure and use of personal information. The CBA recently provided its comments on C-13 before Parliamentary Committee[2] and recommended that one oversight body be created to monitor the cumulative impact of various laws and state actions upon individual privacy. We reiterate that recommendation here. With the proliferation of legislation governing the disclosure of personal information, such a body is essential to ensure a consistent and reasoned approach and to bolster public confidence in the regime established to protect the individual right to privacy.

Our recommendations pertaining to Bill S-4 are as follows:

1. Delete proposed PIPEDA s. 6.1, which provides criteria for "valid consent" and is largely redundant.

2. Amend proposed PIPEDA ss. 7(1)(b.2) and 7(2) (b.2) related to "work product exception", as suggested, to narrow their scope.

3. Conduct further analysis of proposed PIPEDA s. 7(3)(d.1) with a view to narrowing its scope; remove the words "that has been, is being or is about to be committed" from s. 7(3)(d.1) for consistency with existing s. 7(1)(b); and amend s. 7(3)(d.2), related to disclosure without consent, as suggested.

4. Elder Law and Privacy and Access Law Sections recommend deletion of proposed PIPEDA section 7(3) (d.3), related to disclosure without consent where financial abuse is suspected; or if retained recommends amendments to i) specify the government institutions to which the bank may disclose; ii) define the terms "next

---

2 www.cba.org/CBA/submissions/2014eng/14_33.aspx

of kin" and "authorized representative"; iii) require banks to inform customers of their authority to disclose confidential information when abuse is suspected; and iv) require banks to ask customers to whom they would want the bank to disclose their personal information if abuse was suspected. The CCCA supports the proposed provision as drafted in Bill S-4.

5. Consider broadening the kind of information that can be disclosed once a business transaction is completed in proposed PIPEDA section 7.2(2); amend the notice requirement after completion of transaction to qualify the obligation.

6. With respect to breach notification:

   - preserve the threshold for notification to individuals as being "a real risk of significant harm" but revise the threshold for reporting to the Privacy Commissioner such that is based on a "major" or "material" breach threshold;

   - for the purposes of assessing if there is a "real risk of significant harm" to the individual, include the factor of probability of *access* instead of, or supplementary to, probability of *misuse*;

   - delete from the definition of "significant harm" the non-exhaustive list of examples, as effectively being deemed to be "significant", and address that issue in OPC guidelines;

   - exclude any requirement to include non-factual and/or speculative assessments of harm in individual notifications to individuals or reports to the Commissioner;

   - make the power discretionary for an organization who has suffered a breach to notify third party organizations or government institutions (e.g. "may" instead of "shall"), allowing for an assessment of the situation on a case-by-case basis, with the expectation that the OPC would issue guidance in consultation with stakeholders per its existing practice;

   - remove the requirement to keep records and provide guidance regarding what constitutes an acceptable record and, similarly, an acceptable record keeping practice, for privacy breaches; and

   - do not introduce new offences regarding breaches.

7. Conduct further analysis of proposed PIPEDA section 17.1 related to compliance agreements.

III. VALID CONSENT

The consent regime under PIPEDA has functioned well and proven to be adaptive to evolving individual expectations and business practices and technologies. Bill C-12, the predecessor to Bill S-4, proposed a new "valid consent" provision that we understand was intended to help protect the personal information and privacy of minors. Clause 5 of Bill S-4 includes a revised

"valid consent" provision (PIPEDA, s. 6.1), much improved by shifting from a problematic subjective standard to a more appropriate objective standard.

The CBA understands the concerns underlying this proposed amendment to the consent regime under PIPEDA. However, we question whether there is a strong and compelling case for the change, particularly in light of the confusion it may cause. The current requirement to obtain consent in PIPEDA contains a clear statement, in s. 4.3.2 of Schedule 1, that the principle includes "knowledge and consent":

> The principle requires "knowledge and consent". Organizations shall make a reasonable effort to ensure that the individual is advised of the purposes for which the information will be used. To make the consent meaningful, the purposes must be stated in such a manner that the individual can reasonably understand how the information will be used or disclosed.

PIPEDA currently requires that consent be reasonably understandable by the individual. The proposed amendment is mostly redundant in light of this, and risks causing confusion by essentially making the same statement in two different ways.

Introducing a new valid consent obligation could upset the delicate balance that has emerged, over more than a decade, when obtaining consent in different scenarios. Further, the valid consent standard could have the unintended consequence of throwing into question every consent gathered by every organization, from every individual – not just from children. We can see no public policy reason or need for this proposed amendment.

RECOMMENDATION

The CBA recommends that proposed PIPEDA s. 6.1 be deleted from Bill S-4.

IV. WORK PRODUCT EXCEPTION

The CBA questions the possible breadth of the "work product exception" in new PIPEDA ss. 7(1)(b.2) and 7(2)(b.2), proposed in clauses 6(3) and (5) of Bill S-4, which allow the collection and use of personal information without the individual's knowledge and consent if:

> ..it was produced by the individual in the course of their employment, business or profession and the [collection/use] is consistent with the purposes for which the information was produced;

A work product exception to the definition of "personal information" is generally understood to encompass non-sensitive personal information incidentally created in the course of one's employment, business or profession that the individual was hired or retained to produce. We can see scenarios where the broad language of proposed ss. 7(1)(b.2) and (2)(b.2) could be abused. An employee's keystrokes on a computer, records of comings and goings, images on covert video surveillance are all personal information "produced by the individual in the course of employment". If it is legitimate to collect and use this sort of information without the knowledge of the individual, its collection and use is already adequately covered under PIPEDA ss. 7(1)(b) and 7(2)(d).

If these provisions are retained, they should be restricted to personal information that the individual is contracted to produce and with the knowledge of the individual. We propose that the new ss. 7(1)(b.2) and (2)(b.2) be amended as follows:

> ... it was produced <u>with the knowledge of</u> the individual in the course of their employment, business or profession, <u>the personal information is incidental to the work product</u> and the [collection/use] is consistent with the purposes for which the <u>work product</u> was produced;

These amendments would restrict the exception to circumstances where the individual is aware of the personal information being produced, the personal information is incidental to the work product (and not the work product itself) and the purposes for the collection and use of personal information are consistent with the purposes for which the work product was originally produced. For example, notes created during a job interview would incidentally include information about the interviewer as well as the applicant. The organization should be able to deal with the interview notes without the interviewer's consent, but remain subject to all other limitations under PIPEDA with respect to the applicant.

RECOMMENDATION

The CBA recommends that proposed PIPEDA ss. 7(1)(b.2) and 7(2)(b.2) be amended to narrow their scope.

V. DISCLOSURE WITHOUT CONSENT

New PIPEDA sections 7(3)(d.1) and (d.2), proposed in clause 6(10) of Bill S-4, would permit an organization to disclose personal information without the consent of the individual concerned.

While the concept is consistent with previous CBA recommendations[3], the breadth of the new provisions as currently drafted needs to be finessed.

Proposed PIPEDA sections 7(3)(d.1) and (d.2) read as follows:

> Disclosure without knowledge or consent
>
> 7(3) For the purpose of clause 4.3 of Schedule 1, and despite the note that accompanies that clause, an organization may disclose personal information without the knowledge or consent of the individual only if the disclosure is …
>
> > (d.1) made to another organization and is reasonable for the purposes of investigating a breach of an agreement or a contravention of the laws of Canada or a province that has been, is being or is about to be committed and it is reasonable to expect that disclosure with the knowledge or consent of the individual would compromise the investigation;
> >
> > (d.2) made to another organization and is reasonable for the purposes of detecting or suppressing fraud or of preventing fraud that is likely to be committed and it is reasonable to expect that the disclosure with the knowledge or consent of the individual would compromise the ability to prevent, detect or suppress the fraud;

This permits disclosures in certain circumstances but does not compel any disclosures.

A. Consistent with Previous CBA Recommendation

The new sections appear to be connected to the removal of the concept of "investigative bodies" from PIPEDA. Under the investigative body scheme, the Governor in Council could approve (by regulation) specific bodies or categories of bodies to which organizations could disclose personal information under defined circumstances. The proposed new sections are consistent with the expressed position on this issue in earlier CBA submissions:

> The CBA Section recommended [in our 2005 submission]:
>
> - eliminating the investigative body designation process;
> - adopting the Alberta and BC PIPAs' approach, so the right to collect would include a reciprocal right to disclose;
> - adopting the PIPAs' approach so collection, use and disclosure without consent would be permitted if for the purposes of an investigation (i.e.

[3] As noted in previous submissions on PIPEDA reform in 2005, 2006 and 2008: www.cba.org/CBA/submissions/pdf/05-34-eng.pdf, www.cba.org/CBA/submissions/pdf/06-37-eng.pdf, www.cba.org/CBA/submissions/pdf/08-06-eng.pdf.

there is no requirement that a person meet the investigative body requirement for the exemption, and no need to apply to be designated as same); and

- adopting the PIPAs' more express approach to third party processing, so the definition of an organization would include any person working on behalf of that organization, such that in this context an investigator would be considered an agent of their client.

In addition to the anomalies inherent in the current investigation provisions of PIPEDA, the CBA Section believes that the application process to become an investigative body is so onerous, given the prohibitive cost of developing and submitting the application, that it is practically unavailable to all but the most well-funded organizations. By adopting reciprocal disclosure rules and the provisions regarding investigations, distortions that have occurred as a result of a need to qualify as an investigation body would be alleviated.

We strongly agree with conclusion in the Government Response that further examination of the approaches taken by Alberta and BC is required, and that further consideration be given to how best to streamline PIPEDA's investigation provisions to make the process both more effective and logical, and to allow better harmonization with the provinces and territories.[4]

We appreciate that Bill S-4 replaces the investigative body paradigm with the model of reciprocal collection, use and disclosure exemptions.[5]

B. The Need for Finesse

However, the scope of the reciprocal collection, use and disclosure consent exemptions may require some finesse. As currently drafted, the addition of sections 7(3)(d.1) and (d.2) could permit disclosure of personal information in an unnecessarily and inappropriately broad range of circumstances. A "breach of an agreement" can include insurance fraud on one hand, or the trivial violation of the terms of use of a website on the other. A "contravention of the laws of Canada or a province" can range from criminal matters to allegations of copyright infringement.

The organization permitted to make a disclosure without consent under the amended provisions is also not restricted to an organization that is the victim of the legal or contractual breach. Finally, there is no restriction on the kind of information that can be disclosed. In our view, the proposed section 7(3)(d.1) is too broad and can be readily used in circumstances

---

4 www.cba.org/CBA/submissions/pdf/08-06-eng.pdf, p. 16

5 However, the consent exemption for "use" in existing s. 7(2) should also reference a breach of agreement, to be consistent.

where the disclosure of personal information is disproportionate to the alleged contractual or legal violation. In addition, the individual involved is never notified of the disclosure, either at the time of the disclosure or later.

These ambiguities on the scope of the consent exemptions, and the resulting challenges they present, are also present in the BC *Personal Information Protection Act* (PIPA) and the Alberta PIPA, as well as the pending Manitoba *Personal Information Protection and Identity Theft Prevention Act.*[6] However, Bill S-4 presents an opportunity to implement more considered and accountable reciprocal consent exemptions that facilitate the collection, use and the disclosure of personal information in connection with investigations with reasonable limitations. The CBA recommends that the proposed amendments be improved with this objective in mind, and would be pleased to participate in further consultations to develop the improvements.[7]

We understand the need for proposed s. 7(3)(d.2), as major industries in Canada such as banking, financial services, insurance and other private and public sector organizations share information through specialized agencies to detect, suppress and investigate fraud. While fraud is a specific offence that presents a much higher threshold than breach of an agreement or an unspecified contravention of the law, we are of the view that this provision should be more closely tailored to its actual purpose to prevent abuse of its broad wording.

The CBA recommends that s. 7(3)(d.2)be amended as follows:

> **Disclosure without knowledge or consent**
>
> **7(3) For the purpose of clause 4.3 of Schedule 1, and despite the note that accompanies that clause, an organization may disclose personal information without the knowledge or consent of the individual only if the disclosure is …**
>
> **(d.2) made to another organization <u>or part of an organization</u> and is reasonable for the purposes of detecting or suppressing fraud or of preventing fraud that is likely to be committed and it is reasonable to expect that the disclosure with the knowledge or consent of the individual would compromise the ability to prevent, detect or suppress the fraud<u>, provided that the prevention, detection or suppression of</u>**

---

6 Although to the credit of the drafters, Bill S-4 does not include the even more ambiguous criterion in the Alberta PIPA and the pending Manitoba *Personal Information Protection and Identity Theft Prevention Act*, for an "investigation" of "circumstances or conduct that may result in a remedy or relief being available at law."

7 The words "that has been, is being or is about to be committed" should be removed from 7(3)(d.1), to be consistent with complimentary existing s. 7(1)(b).

> **fraud is among the principal objects of the other organization or part of the organization;**

This amendment would limit the disclosure to organizations or specialized groups within organizations such as corporate security or fraud prevention groups that are charged with the prevention, detection or suppression of fraud, and that typically abide by very strict procedures.

RECOMMENDATION

> **The CBA recommends that proposed PIPEDA s. 7(3)(d.1) be subject to further analysis, with a view to narrowing its scope; the words "that has been, is being or is about to be committed" be removed from s. 7(3)(d.1), to be consistent with complimentary existing s. 7(1)(b); and that s. 7(3)(d.2) be amended as suggested.**

VI. DISCLOSURE WITHOUT CONSENT-FINANCIAL ABUSE

Bill S-4, clause 6(10) amends PIPEDA section 7(3) to permit disclosure of personal information by an organization without the knowledge or consent of its customers, when such disclosure is:

> *(d.3*) made on the initiative of the organization to a government institution, a part of a government institution or the individual's next of kin or authorized representative and
>
> > (i) the organization has reasonable grounds to believe that the individual has been, is or may be the victim of financial abuse,
> >
> > (ii) the disclosure is made solely for purposes related to preventing or investigating the abuse, and
> >
> > (iii) it is reasonable to expect that disclosure with the knowledge or consent of the individual would compromise the ability to prevent or investigate the abuse;

There are divergent views in the CBA on this provision. The Elder Law and Privacy and Access Law Sections recommend that it be deleted or, at a minimum, amended. The Canadian Corporate Counsel Association (CCCA) approves it as drafted.

In the view of the CBA Elder Law and Privacy and Access Law Sections, the proposed amendments raise two concerns:

1) The statutory waiver of consent in s. 7(3)(d.3) is intended to apply to older adults and, as such, may be discriminatory; and

2) The list of people and organizations that may receive disclosure without consent is unnecessarily broad and unspecified. In particular, the amendment to disclose

> information to "next of kin" or "authorized representatives" is problematic as financial abusers of older adults are most often people that could be described as "next of kin" or "authorized representatives".

The Canadian Bankers Association has urged Industry Canada to adopt these proposed amendments, noting its concerns about financial abuse with particular regard to seniors in 2008 and 2014 submissions.[8] While the proposed section does not apply exclusively to banks or to older adults, will have a disproportionate and negative, unintended impact on older adults in managing their financial affairs.

First, the right to privacy and the application of the fair information obligations in PIPEDA should apply equally to all banking customers, regardless of age. An individual is free to make decisions about their finances, unless and until found to lack capacity to manage their property.

Second, the list of individuals and organizations that the bank may notify of its concerns is unnecessarily broad, and potentially harmful. The perpetrators of financial abuse, particularly the financial abuse of older adults, are often "next of kin" or "authorized representatives".[9] Disclosure of information to "next of kin" or "authorized representatives" without the knowledge or consent of the alleged victim, as contemplated in s. 7(3)(d.3), may alert the perpetrator to the bank's awareness of the abuse, which may increase the likelihood of further harm to the alleged victim. The lack of definition of "next of kin" and "authorized representative" means that bank clients would have no prior notice of whom reports of alleged abuse could be made to.

Financial abuse, whether in the in the form of theft, extortion, or fraud, is a crime and should be reported to the police. Police would be captured by the phrase "government institution or "part of a government institution" in s. 7(3)(d.3). It also captures reports by banks to Offices of the Public Guardian and Trustee in provinces, such as Ontario, where legislation permits reporting of alleged financial abuse of mentally incapable adults (once incapacity is established). Legislation in other provinces permits or requires reporting of financial abuse to a government

---

8 www.cba.ca/contents/files/submissions/sub_20080117_01_en.pdf,p. 8; www.fin.gc.ca/consultresp/fcpf-cpcpsf/073-fcpf-cpcpsf.pdf, p. 11

9 *R. v. Kaziuk*, 2011 ONCJ 851; *R. v. Webb*, 2011 SKPC 181; *R. v. Taylor*, 2012 ONCA 809; *Nguyen-Crawford v. Nguyen*, 2010 Carswell Ont 9492; *Johnson v. Huchkewich,* 2010 Carswell Ont 8157; *McMaster v. McMaster*, 2013 ONSC 1115; see also Law Commission of Ontario, "A Framework for the Law as it affects Older Adults: Advancing Substantive Quality of Older Persons through Law, Policy and Practice" (Toronto: April 2012); Alberta Law Reform Institute, "Enduring Powers of Attorney: Safeguards Against Abuse" (Edmonton: February 2003).

agency and those communications by banks could be encompassed by s. 7(3)(d.3). However, the PIPEDA amendment does not sufficiently specify the individuals and organizations that a bank may report to and, as such, is too broadly drafted.

The Elder Law and Privacy and Access Law Sections recommend that s. 7(3)(d.3) be deleted from Bill S-4. If it is retained, they recommend the following amendments:

1) the government institutions to which the organization may disclose be specified;
2) the terms "next of kin" and "authorized representatives" be defined;
3) the provision require an organization to inform customers of their authority to disclose confidential information when abuse is suspected; and
4) the provision require an organization to ask customers to whom they would want the organization to disclose their personal information if abuse was suspected.

The CCCA, on the other hand, is satisfied with s. 7(3)(d.3) as drafted, without amendment. They see a very real need for a limited exception to enable organizations to deal with vulnerable persons (including older adults) who may fall victim to financial abuse. Financial abuse of any vulnerable person (whether an older adult, a person with disability, a newcomer or any other person who may be vulnerable due to a lack of financial literacy in a given situation) is complex and the problem has been recognized by the government, as well as private and public sector organizations, as an area of growing concern.[10]

In the CCCA's view, the provision is adequately drafted to give organizations flexibility, without violating PIPEDA, to communicate circumstances to government entities, next of kin or authorized representatives, where a person may be at risk of financial abuse. Situations facing organizations will vary from case to case, and the discretion to disclose without consent is adequately tempered by the requirement that the organization have reasonable grounds.

Since the government's review of PIPEDA began in 2005, the banking industry and others have sought an amendment to PIPEDA to allow disclosure to lawful authorities, next of kin or other authorized representatives of personal information related to potential financial abuse. Currently PIPEDA allows banks to report suspected abuse to relevant authorities, such as police or the Public Guardian and Trustee office, where an organization has reasonable grounds to

---

10 www.ifa-fiv.org/wp-content/uploads/2013/03/Jane-Rooney-Financial-Abuse-of-Seniors.pdf; www.bcli.org/sites/default/files/CCEL_Background_Paper_Financial_Elder_Abuse_2013_0.pdf; www.ifa-fiv.org/wp-content/uploads/2013/11/Financial-Abuse-of-Seniors-Meeting.pdf; www.seniorscouncil.gc.ca/eng/research_publications/elder_abuse/2007/hs4_38/page06.shtml

believe a law is being contravened. If no law is being contravened, however, organizations are constrained by PIPEDA on what actions they can take even if abuse is suspected.

The CCCA does not believe there is a need to define "authorized representatives" or "next of kin", and does not share the Elder Law Section's concerns. The terms can be factually determined case-by-case in practice. The CCCA does not believe it is practical to define these terms in legislation, or that it should to require persons to identify in advance to whom financial abuse should be reported.

RECOMMENDATION

The Elder Law and Privacy and Access Law Sections recommend deletion of proposed PIPEDA s. 7(3) (d.3) or, if retained, amendments be made to i) specify the government institutions to which the bank may disclose; ii) define the terms "next of kin" and "authorized representative"; iii) require banks to inform customers of their authority to disclose confidential information when abuse is suspected; and iv) require banks to ask customers to whom they would want the bank to disclose their personal information if abuse was suspected. The CCCA supports the proposed provision as drafted in Bill S-4.

VII. BUSINESS TRANSACTION EXCEPTION

Bill S-4, clause 7 proposes new consent exceptions in PIDEDA in the context of business transactions. The CBA previously recommended an exception for information disclosed in the course of a business transaction, with appropriate safeguards in place, and supports this amendment, subject to the recommendations below.[11]

In analyzing the proposed amendments, we looked to differences between the amendments in Bill S-4 for business transactions and equivalent sections of the BC and Alberta PIPA[12]. Our analysis is divided into three parts, in keeping with the framework of Bill S-4 and its provincial counterparts: disclosure prior to the transaction taking place; use of information if the transaction proceeds; and notice requirements after the transaction is completed.

---

11 www.cba.org/CBA/submissions/pdf/05-34-eng.pdf, p. 18-19

12 We cite the Alberta PIPA legislative scheme, recognizing that as a result of the Supreme Court of Canada's decision in *Alberta (Information and Privacy Commissioner) v. United Food and Commercial Workers, Local 401* [2013] 3 S.C.R. 733, the *Personal Information Protection Act*, S.A. 2003 c.P-6.5 ("Alberta's Privacy Act"), was declared invalid with the declaration suspended for one year from the date of the decision of November 15, 2013 to allow the Alberta legislature to bring the legislation into compliance with the Charter.

A. Disclosure prior to a transaction taking place

The proposed PIPEDA s. 7.2 (1) permits disclosure of personal information between the parties to a prospective business transaction as long as certain conditions are met, including an agreement between the organizations involved that sets out conditions on use and protection of the information. This form of agreement is a critical component to disclosure of personal information in these circumstances. It does not enumerate about whom the information can be disclosed in the prospective business transaction.

By contrast, BC PIPA permits disclosure of personal information only about employees, customers, directors, officers or shareholders (section 20(2)). Alberta PIPA is akin to Bill S-4 and does not enumerate categories of individuals but speaks to disclosure of data related to identifiable individuals (section 22(3)). We support the approach in Bill S-4. In our view, there is little practical difference between the two approaches as a business is unlikely to have personal information about individuals who are not "employees, customers, directors, officers and shareholders". As noted in our 2005 submission, these individuals would be expected to know that their personal information may be disclosed in the course of a business transaction and obtaining consent is frequently impractical and inappropriate in this context. [13]

B. Use of information if the transaction proceeds

Once the business transaction is completed, proposed PIPEDA s. 7.2(2) would allow parties to the transaction to use and disclose personal information disclosed under s. 7.2(1) without the knowledge and consent of the individuals, if certain steps are followed. The section suggests that personal information not disclosed under 7.2(1), because it was not necessary to complete the transaction, cannot be disclosed and used after the transaction is completed.

This approach is unnecessarily restrictive. In practice, different information may be required to prepare for rapid, post-closing transition to new owners than was needed initially to complete the transaction. Neither Alberta PIPA nor BC PIPA limits use of information (without consent) post-closing to the information disclosed before the transaction was completed, subject to requirements to (i) enter into an agreement to use and disclose the information only for the purposes for which it was originally collected, and (ii) limit use without consent to information

---

13 www.cba.org/CBA/submissions/pdf/05-34-eng.pdf, pp. 18-19

relating solely to carrying on the business or activity for which the transaction took place.[14] We recommend that disclosure of information be permitted, post-closing, beyond that already disclosed before the transaction was completed, subject to protections like those listed above.

C. Notice requirements after the transaction is completed

If the business transaction is completed, proposed PIPEDA section 7.2(2)(c) requires that the individual be notified of the transaction and the fact that their personal information was disclosed. BC's PIPA includes a similar requirement in section 20(3)(c). There is no general requirement in Alberta's PIPA to notify individuals after the transaction is completed.

The CBA supports the inclusion of a notice provision but recommends that the obligation be qualified to require notice "where it is practicable to do so" and "in a manner reasonable to the circumstances", which reflects current practices and alleviates the administrative burden of discharging an unqualified requirement.

RECOMMENDATION

The CBA recommends that the kind of information that can be disclosed once a business transaction is completed, in proposed PIPEDA s. 7.2(2), be broadened; and that the notice requirement after completion of the transaction, in proposed s. 7.2(2), be qualified.

VIII. BREACH NOTIFICATION

In past CBA submissions on proposed amendments to PIPEDA,[15] the proposal to introduce a breach notification and reporting regime has been of particular interest. We are particularly keen to avoid the U.S. experience with a multitude of approaches at the federal and state levels creating a patchwork of laws. The public interest is not well served by inconsistent requirements, which can result in unnecessary complexity and confusion for the public and organizations. We are aware of the spectrum of options and have advocated for a balanced approach that requires breach notification to individuals in some circumstances and reporting to the Office of the Privacy Commissioner of Canada in other, slightly narrower, circumstances.

---

14 Alberta *PIPA*, s. 22(1) to (5); B.C. *PIPA* s. 20(3).

15 *Supra*, footnote 3

The approach adopted in Bill S-4 is, in a number of respects, consistent with the 2008 CBA submission[16]. Specifically:

- the proposed regime to introduce an explicit obligation to notify individuals, and report to the Office of the Privacy Commissioner of Canada (OPC), is consistent with the general PIPEDA framework;
- it is flexible and allows for additional specificity via regulations (e.g. timing, form and manner, level of information, etc.) and the development of guidelines, as necessary; and
- it contains an exception to the informed consent requirement that requires organizations to notify certain third party organizations or government institutions in certain circumstances when there has been a breach.

However, Bill S-4 differs from the CBA recommendations in at least two material respects:

- First, different threshold criteria should be established for notifying individuals and reporting to the OPC, to meet the different objectives of these two obligations.
- Second, consistent with the general approach in PIPEDA and the ongoing reliance on the "reasonable person" test, failure to notify or report should not constitute an "offence" under PIPEDA, as proposed in s. 24 of Bill S-4. However, similar to other acts of non-compliance under PIPEDA, non-compliance with the notification and reporting requirements should be subject to the general PIPEDA complaint regime and remedies available pursuant to application to the Federal Court, including the ability to order the payment of damages or changes to an organization's practices.

We recommend some changes to improve the effectiveness of a breach notification regime.

A. Recommended improvements to breach notification regime

Subject to the recommended improvements, the CBA generally supports the proposed breach notification and reporting regime in Bill S-4, which is consistent with the overall framework of PIPEDA. The approach will further entrench an organization's obligation to safeguard personal information, will require meaningful notice to individuals when appropriate and, assuming that our recommendations are adopted, will ensure that certain key material security breaches are reported to the OPC.

16 www.cba.org/CBA/submissions/pdf/08-06-eng.pdf

Notification and Reporting Thresholds

Bill S-4. s. 10 sets out the same test for notification of a breach to the individual and reporting of breaches to the Privacy Commissioner: where "it is reasonable in the circumstances to believe that the breach creates a real risk of significant harm to the individual."[17] In other words, every breach which is notifiable to the individual is also reportable to the Privacy Commissioner. This is unnecessary and, in our view, should not be required. While the approach in Bill S-4 is similar to the Alberta PIPA, it deviates from the balanced and widely supported approach in former Bill C-12, and current guidance from the OPC regarding breaches.

The 2008 CBA submission noted[18]:

> The Government addressed Recommendations 23, 24 and 25 of the Report in its Response. To paraphrase:
>
> - for a certain defined category of breaches where a *high risk of significant harm* exists, there should be a statutory requirement for prompt notification of individuals affected by the breach;
> - there should be a statutory requirement to report any *major loss or theft* of personal information to the Privacy Commissioner within a specified period of time; [emphasis added]
>
> …
>
> While formulated somewhat differently, both approaches suggest notification criteria based on an assessment of the potential risk of harm for the individual, considering the sensitivity of the information in question and the probability that the information would be accessed.
>
> In its response to Recommendation 23, the Government also enumerated purposes for which the Commissioner would receive reports of a major loss or theft of personal information (collectively, the "Reporting Purposes"):
>
> - to allow for oversight of organizational practices
> - to track the volume and nature of breaches
> - to track the steps taken by organizations respecting the notification process when that process is required, and

---

17 Proposed s. 10.1(1) in PIPEDA.

18 In connection with the Industry Canada consultation on the Government Response to the Fourth Report of the Standing Committee on Access to Information, Privacy and Ethics on the Personal Information Protection and Electronic Documents Act (PIPEDA). www.parl.gc.ca/HousePublications/Publication.aspx?DocId=3077726&Mode=1&Language=E

- to assist small and medium-sized enterprises (SMEs), that may lack the internal resources necessary to make notification assessments regarding the notification process.

> The Government Response effectively recommends a dual obligation model. Organizations determine the need for notification if there is a "high risk of significant harm" to individuals, and must report the breach to the Commissioner if the "major loss or theft" threshold is met.[19]

The Government Response recommended, and the CBA agreed, that in light of the different objectives of notification and reporting, the threshold in each case should be different.

The Parliamentary Committee Report specifically noted that in determining the threshold for when an organization should be required to report a breach to the Privacy Commissioner:

> …we do not wish to see the Office of the Privacy Commissioner overburdened with breach reporting. Certainly, requiring notification to the Office of the Privacy Commissioner in every instance of a security breach may create an unworkable burden on that Office, and, at least, will have significant resource implications. We suggest that careful consideration be given to this issue in the development of a breach notification provision in PIPEDA[20]

Between the Report and the Government Response, then, there appeared to be consensus, notwithstanding the oversight role of the Commissioner proposed by the government, that a privacy breach must meet a threshold for it to be reported to the Commissioner.

Again, given that the purpose of reporting to the Commissioner (to track the volume and nature of breaches) is different from the purpose for notification (harm mitigation for each subject individual), the CBA agreed with the Government Response that there should be different thresholds for notification and reporting, which reflected those differing objectives. While the threshold for notifying individuals should be based on the existence of a high risk of harm (or as in Bill S-4, a "real risk of significant harm") to an individual, reporting to the OPC should be premised on the existence of a major (or as in former Bill C-29, a "material") breach.

Another consequence of the reporting threshold being related only to the degree of harm to an individual is that breaches which may not meet that threshold, but which are problematic because of the number of individuals involved or because they may evidence a systemic

---

19 www.cba.org/CBA/submissions/pdf/08-06-eng.pdf, pp. 2-4

20 www.parl.gc.ca/content/hoc/Committee/391/ETHI/Reports/RP2891060/ethirp04/ethirp04-e.pdf, p. 44

problem, will not be reported to the Commissioner. The 2008 CBA submission reviewed in detail the factors contributing to the different notification and reporting thresholds, and for the reporting threshold specifically noted that:

> The number of individuals affected by a breach may also be a determining factor in whether to report a breach. Clearly, to meet the "major loss" threshold criterion, an incident where only a single individual is affected would likely not require reporting. However, if a pattern of similar breaches of information occurred over a period of time, reporting may well be appropriate. For example, if the number of individuals affected is low, but the sensitivity and probability of access are both high, reporting might be required, particularly if there was a pattern of multiple incidents with similar characteristics that might indicate a systemic problem within the affected organization.[21]

The CBA recommends that the threshold for notification to individuals be preserved as being "a real risk of significant harm" but that the threshold for reporting to the OPC be based on a "major" or "material" breach threshold.

"Probability of access"

The CBA supports the proposed amendment to base the decision to notify an individual on an assessment of whether the breach creates a "real risk of significant harm" to the individual.[22] We recommend that, in addition to factoring in the sensitivity of the personal information as required in proposed PIPEDA, s. 10.1(8),[23] the second factor should be probability of *access*, rather than probability of *misuse.*

The 2008 CBA submission reviewed the relevance of the twin factors of sensitivity and access, which are equally relevant today:

> In its 2005 submission, the CBA Section … referred to California's SB 1386, where a duty to notify is imposed if two thresholds are met:
>
> - Insufficient encryption: The information is (a) unencrypted or otherwise unprotected so there is no reasonable assurance that the information is inaccessible, or (b) encrypted or otherwise so protected, but the organization has received notice that the protection has been breached; and

---

21 www.cba.org/CBA/submissions/pdf/08-06-eng.pdf, pp. 6-7

22 Proposed s. 10.1(3) in PIPEDA, Bill S-4, s. 10.

23 Bill S-4, s. 10

- Information is sensitive: The information falls in a specified category of types of sensitive personal information [e.g. Social Insurance Numbers, sensitive financial information (including bank account numbers, credit card numbers, and associated passwords and PINs) and health information].

In its white paper on the issue, the Canadian Internet Policy and Public Interest Clinic recommended a similar balanced approach where notification would be required if "designated personal information" has been or is reasonably believed to have been acquired by an unauthorized person. The term "designated personal information" is defined to:

- include government issued ID numbers (SIN, drivers' licence numbers or health card numbers) and account numbers, credit or debit card numbers; and
- exclude information that is encrypted, redacted or otherwise altered by any method or technology in such a manner that the name/data elements are unreadable by unauthorized persons.

While formulated somewhat differently, both approaches suggest notification criteria based on an assessment of the potential risk of harm for the individual, considering the sensitivity of the information in question and the probability that the information would be accessed.[24]

In many cases, an organization subject to a breach of security safeguards can reasonably determine the probability of access to the information, by assessing the extent to which the information was "encrypted, redacted or otherwise altered". Determining the likelihood of misuse is more challenging, as it requires both an assessment of probability of access, and of whether the data will be "misused" when accessed. The latter factor may be difficult, if not impossible, for an affected organization to assess, without knowledge of the parties perpetrating the breach. It would be more reasonable and more practical for "probability of misuse" to be one of the factors, with "probability of access" as an independent, standalone consideration.

Definition of "significant harm"

In determining whether a breach is notifiable and reportable, Bill S-4, s. 10 sets out (a) the test of "real risk of significant harm", and (b) a definition of "significant harm", consisting of a non-exhaustive list of examples.[25]

---

24 www.cba.org/CBA/submissions/pdf/08-06-eng.pdf, pp. 3-4

25 Proposed PIPEDA s. 10.1 (7), Bill S-4, s. 10

We question whether the latter definition should be included. While some listed examples unquestionably constitute "significant harm" (e.g. bodily harm, loss of employment), others would not necessarily constitute "significant" harm, depending on the severity of the circumstances (e.g. damage to relationships or damage to property). While the examples are all forms of harm, whether they are "significant" would often depend on the context. Rather than deeming all the listed harms to be significant, consideration should be given to deleting the definition and allowing the OPC to issue guidelines, or changing the definition to allow for an assessment of context.

Contents of Notification

The 2008 CBA submission noted:

> The CBA Section encourages an approach to reporting where the contents of a report to the Commissioner are based simply on facts. The BC Information and Privacy Commissioner's Privacy Breach Reporting Form (November 2006) asks for general information about the facts of the breach. The same form also asks the organization to identify types of harm that may result from the breach, which is speculative and may actually discourage proactive reporting. In contrast, a factually based form will encourage reporting. In our view it should be developed by the Commissioner in collaboration with all stakeholders.[26]

Similarly, Alberta PIPA, s. 19 requires that privacy breach reports to the Privacy Commissioner include "an assessment of the risk of harm to individuals as a result of the loss or unauthorized access or disclosure".[27]

While the content of the notice to the individual and report to the Privacy Commissioner have yet to be prescribed, we recommend not requiring notices and reports to include speculative assessments of the risk of harm which, among other issues, are potentially prejudicial for the notifying/reporting organization, for example where an individual may claim damages against the organization based on a privacy breach.

Notification to third party organizations

Bill S-4 would create a new exception to the informed consent requirement, enabling organizations to notify third party organizations or government institutions of a breach where

---

26 www.cba.org/CBA/submissions/pdf/08-06-eng.pdf, p. 7

27 *Personal Information Protection Act,* SA 2003, c P-6.5, s. 19 (http://canlii.ca/t/522mh)

the third party organization or government institution may be able to reduce the risk of, or mitigate, the harm that could result from the breach.[28] Bill S-4 casts this exception as a positive obligation of an organization that has experienced a breach to notify appropriate third parties, where the organization notifies affected individuals of the breach.

Although similar to what was contemplated in the 2008 CBA submission, Bill S-4 takes a broader approach. The 2008 CBA submission suggested granting a discretion, or even imposing an obligation, on organizations to notify credit bureaus of potential fraud risks connected with a breach, following consultation with the credit bureaus and groups that represent credit grantors. It acknowledged that there may be a rationale for including notification to other organizations well placed to assist in the prevention of fraud.

A broad obligation in PIPEDA to notify appropriate third parties is a potentially useful tool for organizations proactively taking steps to protect individuals whose personal information has been compromised, without losing valuable time to first secure consent to further disclosure. However, a mandatory rather than permissive requirement to notify third parties raises some serious issues:

- What obligation, if any, does an organization or government institution receiving the notification have to take steps to reduce the risk of, or mitigate, the harm that could result from a breach?
- What obligation does the organization that suffered the breach have to compensate the third parties for costs associated with taking such steps?
- What are the consequences, if any, for an organization that fails to identify every third party organization or government institution that may be in a position to reduce or mitigate the harm?

The CBA recommends that the proposed PIPEDA, s. 10.2(1) in Bill S-4 be amended to make the power to notify third party organizations or government institutions discretionary (e.g. "may" instead of "shall"), allowing an assessment on a case-by-case basis, with the expectation that the OPC would issue guidance in consultation with stakeholders on its existing practice[29].

---

28 Proposed PIPEDA s. 10. 2(1), Bill S-4, s. 10

29 See the OPC's *Key Steps for Organizations in Responding to Privacy Breaches* www.priv.gc.ca/information/guide/2007/gl_070801_02_e.asp

Record Keeping re Breaches

The record keeping provisions of the proposed breach notification scheme pose practical challenges for organizations.[30] This is our overarching concern. The lack of a specific materiality threshold for reporting breaches to the OPC means that organizations must determine when it is necessary to record a potential breach as a specific event. With no threshold, the reasonable conclusion is that all breaches, regardless of how trivial or inconsequential, must be diligently logged in the prescribed manner.

For example, many organizations adopt a "clean desk policy" to protect personal information from being inadvertently disclosed to others who don't have a need to know. If an employee leaves a document on their desk, this is a technical breach of security safeguards adopted by the organization that would have to be logged, regardless of whether the document was actually exposed to any person. If the employee fails to report it, it is not logged and this failure constitutes an offence under the proposed amendments. Similarly, if someone overhears the conversation of a customer with a pharmacist in a busy drug store, that is a disclosure without consent, requiring logging. Again, failure to log that would be an offence. The likely outcome is that organizations will spend time and resources keeping records of all breaches, regardless of whether they "create a real risk of significant harm" or constitute a "material breach".

This will create significant administrative costs and burdens on organizations as they will need to design robust processes to capture all potential breaches and record them consistently. The design strategy will require some consideration of human capital and who in an organization is best placed to make the necessary determinations and act as record keepers. This impact will be disproportionate for small businesses. Moreover, the proposed amendments are silent on record retention periods, the manner in which records must be designed and maintained, and the level of detail required in the report. There is also no limitation on jurisdiction: are foreign organizations expected to keep records related to the personal information of Canadians and is it intended to give the OPC the power to demand records from organizations outside Canada? What of organizations with customers in Alberta and BC, where no obligation exists? Absent draft regulations or instructive OPC guidelines, it is difficult to know what constitutes an acceptable record and, similarly, an acceptable record keeping practice.

---

30 Proposed PIPEDA, s. 10.3(1), Bill S-4, s.10

We are also concerned about how a "breach of security safeguards" affects an organization that goes beyond the minimum level of security that is appropriate in the circumstances. Bill S-4, clause 2 defines "breach of security safeguards" as:

> ..the loss of, unauthorized access to or unauthorized disclosure of personal information resulting from a breach of an organization's security safeguards that are referred to in clause 4.7 of Schedule 1 or from a failure to establish those safeguards.

A breach is any violation of a company's safeguards. One can imagine an organization with exemplary safeguards that go well beyond the legal minimum. A lapse in those safeguards, even those exceeding the minimum required, would require the same logging as a more substantial lapse. Requiring paperwork (and possible scrutiny by the Privacy Commissioner) for a trivial lapse that carries no risk of misuse of the information provides tangible disincentives to adopt security standards beyond the bare minimum.

The issues on keeping records are particularly problematic as not keeping adequate records would also constitute an offence under the proposed amendments to PIPEDA s. 28[31] The CBA recommends that this requirement be removed from Bill S-4.

B. New Offences and Penalties Not Needed

Contrary to the position recommended in the 2008 CBA submission and the balanced approach in former Bill C-12, Bill S-4 introduces new offences related to the breach notification and reporting provisions. The approach adopted in Bill S-4 is inconsistent with the overall dispute resolution framework in PIPEDA which is overseen by an ombudsperson (the Commissioner) with ultimate recourse to the Federal Court.

The 2008 CBA submission noted that any proposal to introduce specific offences or penalties for failure to notify would raise difficult threshold issues for when a penalty should be imposed. For example, if an organization made a "wrong" decision about its obligation to notify or report, that decision would have been based on several factors that may require exercise of judgment specific to the particular circumstances. The notification requirement articulates the test of reasonability (i.e. "if it is reasonable in the circumstances to believe that the breach creates a

---

31 Bill S-4, s. 24

real risk … to the individual"). The existing overall scheme of PIPEDA contains several references to an obligation to be reasonable, but none serve as the basis for an offence.

Imposing penalties for non-compliance would also be inconsistent with PIPEDA's existing approach to offences and penalties, which address matters involving a significant element of malfeasance (such as obstructing the Commissioner in an investigation or deleting personal information subject to an access request). A "wrong decision" about notification may not be sufficiently egregious to make it an offence at a similar level. If offences for non-compliance were added to PIPEDA, they may require the criminal law burden of proof (beyond a reasonable doubt) which would be inconsistent with the "reasonable" approach articulated by the breach notification and reporting provisions proposed in Bill S-4.

We question whether the experience to date suggests that new offences or penalties are needed to ensure compliance. Currently PIPEDA has no explicit requirement to notify individuals or report material breaches to the Commissioner. Nevertheless, PIPEDA came into effect over a decade ago, notification and reporting has often been voluntarily effected based on an organization's obligation to safeguard personal information, and even more so with the Commissioner's 2007 *Guidelines for Organizations in Responding to Privacy Breaches*.

For these reasons, we do not support the approach taken in Bill S-4 to introducing new offences for failure to notify or report a breach, or for failure to keep adequate records.

RECOMMENDATION

The CBA recommends the following with respect to the proposed "breach notification" provisions:

- **preserve the threshold for notification to individuals as being "a real risk of significant harm" but revise the threshold for reporting to the Privacy Commissioner such that is based on a "major" or "material" breach threshold;**
- **for the purposes of assessing if there is a "real risk of significant harm" to the individual, include the factor of probability of *access* instead of, or supplementary to, probability of *misuse*;**
- **delete from the definition of "significant harm" the non-exhaustive list of examples, as effectively being deemed to be "significant", and address that issue in OPC guidelines;**
- **exclude any requirement to include non-factual and/or speculative assessments of harm in individual notifications to individuals or reports to the Commissioner;**

- **make the power discretionary for an organization who has suffered a breach to notify third party organizations or government institutions (e.g. "may" instead of "shall"), allowing for an assessment of the situation on a case-by-case basis, with the expectation that the OPC would issue guidance in consultation with stakeholders per its existing practice;**

- **remove the requirement to keep records and provide guidance regarding what constitutes an acceptable record and, similarly, an acceptable record keeping practice, for privacy breaches; and**

- **do not introduce new offences regarding breaches.**

IX. COMPLIANCE AGREEMENTS

The CBA is concerned about the "compliance agreements" contemplated in new section 17.1 of PIPEDA, proposed in s. 15 of Bill S-4. Our principal concern is that while entering into such an agreement with the Privacy Commissioner stays any court enforcement by the Commissioner, it does not have any effect on any affected individual's right to go to court against the organization for the same matter under investigation. This omission means that there is a much lower incentive for organizations to enter into such agreements. Also, it is not consistent with the regime in other similar schemes. The CBA recommends further analysis of the rationale for and impact of this provision.

RECOMMENDATION

The CBA recommends that further analysis be conducted of the proposed amendment contemplating compliance agreements.

X. CONCLUSION

The CBA appreciates the opportunity to offer input on Bill S-4, the latest iteration of amendments to PIPEDA. We are generally supportive of the proposed amendments. With the adoption of our recommendations for improvement, Bill S-4 has the potential to strike the right balance between individual privacy rights and the facilitation of commerce in Canada. Please let us know if you have any questions regarding our recommendations or if we can be of any further assistance in the development of this legislation.