PUBLIC INTEREST ADVOCACY CENTRE
LE CENTRE POUR LA DÉFENSE DE L'INTÉRÊT PUBLIC
ONE Nicholas Street, Suite 1204, Ottawa, Ontario, Canada K1N 7B7
Tel: (613) 562-4002. Fax: (613) 562-0007. E-mail: piac@piac.ca. Website: http://www.piac.ca

26 February 2016

VIA EMAIL

Standing Committee on Alberta´s Economic Future
3rd Floor, 9820 – 107 Street NW
Edmonton, AB T5K 1E7

Dear Members of the Standing Committee on Alberta´s Economic Future,

Re: The *Personal Information Protection Act* Review (29th Legislature)

In accordance with the Call for Submission published by the Standing Committee on Alberta's Economic Future, please find enclosed the submission of the Public Interest Advocacy Centre ("**PIAC**") in response to the *Personal Information Protection Act* Review and Discussion Guide.

Thank you for this opportunity to comment.

Yours truly,

[original signed]

John Lawford,
Executive Director and General Counsel

Encl.

*** End of Cover Letter***

Alberta *Personal Information Protection Act* Review
Submission of Public Interest Advocacy Centre (PIAC)

26 February 2016

Introduction

The Public Interest Advocacy Centre (PIAC) is pleased to submit its comments to the Alberta *Personal Information Protection Act* (PIPA) Review. After introducing PIAC and its privacy work, the comments below will be restricted to the topic of data breaches and data breach notifications (Question 17 of the Discussion Guide). PIAC commends the Alberta Office of the Information and Privacy Commissioner (OIPC) on its work in this area, and encourages the OIPC to remain committed to its standards-setting data breach notification laws and practices. Under no circumstances should PIPA be "harmonized" in any way with the federal *Personal Information and Electronic Documents Act* (PIPEDA), as this would represent a dilution and weakening of PIPA, to the detriment of those it means to protect.

About PIAC

PIAC is a federally incorporated non-profit organization and charity that provides legal and research services on behalf of consumers, and in particular, vulnerable consumers. This includes a long history of involvement in Canadian privacy law, in addition to telecommunications, broadcasting, energy, financial services, and consumer protection law. For example, PIAC has published a number of reports with the support of Industry Canada and the Office of the Privacy Commissioner of Canada (OPCC), on topics such as location-based technologies and privacy implications, data breach notification laws, a "Do Not Track" list for Canada, radio frequency identification used by shopping retailers, and use of biometrics in national identification cards. PIAC's work has also prompted several investigations by the OPCC and the CRTC, such as into the youth networking site Nexopia, and Bell Canada's "Relevant Ads" program. In 2014, PIAC appeared before the Senate Standing Committee on Transport and Communications to discuss Bill S-4, the *Digital Privacy Act.*

PIPA Data Breach Notification Provisions Are Effective, Set a Leading Standard, and Should Be Maintained As They Are

The Alberta PIPA provisions on data breach notifications are the best in the country in terms of encouraging notification and protecting potential victims of data breaches, both provincially and federally. This is a direct result of the legal obligation (and penalty-driven financial incentive) that PIPA places on private sector entities to report all serious data breaches to the OIPC (s 34.1), and the subsequent requirement on the OIPC to decide whether the breach necessitates notifying the individuals impacted (s 37.1(1)). As former Commissioner Frank Work said in the 2010-11 OIPC Annual Report, these provisions "make for more uniform reporting, more consistent application of the standard (real risk of significant harm) and better notification where notification was required".[1]

What is essential to, and effective with Alberta PIPA's approach to data breaches is that it helps to avoid the fundamental weakness of its federal counterpart, PIPEDA: PIPA largely removes the element of conflict of interest within companies that have experienced a data breach incident by incentivizing the companies through risk of non-reporting penalties and ultimate review of their harm assessments by the OIPC. This dual process strongly encourages companies to more objectively assess the individual impact of any data breach on particular individuals. This leads to a higher rate of data breach notifications and thus more people who actually are notified and thus able to act on such notice to protect their personal information, reputation, and financial interests. Data breach and notification statistics from various jurisdictions in Canada seem to bear out this observation.

For example, in its 2011 Annual Report, the Alberta OIPC reported a more-than-threefold increase in private sector data breach notifications since section 34.1 and related provisions came into force in May

[1] Office of the Information and Privacy Commissioner of Alberta, 2010-11 Annual Report (2011), online: <http://www.oipc.ab.ca/Content_Files/Files/AnnualReports/AR_2010_2011.pdf>, at pages 5-6.

2010.[2] The benefit to individuals impacted by such data breaches also emerged quickly: in approximately one third of those reported breaches, the organization resisted notifying its customers and the OIPC had to order it to do so.[3]

A report that the OPCC commissioned in 2013, on Canadian businesses and their attitudes and approaches to privacy issues, is similarly illuminating. Half (50%) of business executives surveyed reported being "not at all concerned" about a data breach,[4] and over half the companies included (58%) had no data breach guidelines in place, in the event where customers' personal information is compromised.[5] Furthermore, according to a 2010 EKOS survey involving 1005 businesses in Canada, only 29% of businesses notified their customers in the event of a data breach, while 7% notified privacy government agencies. For businesses that had not experienced data breaches, only 34% of them indicated they would notify impacted individuals in the event of a breach, and 0% would notify privacy government agencies.[6]

The above data demonstrates the immediate impact of and need for PIPA's data breach notification provisions. However, it also highlights two further aspects of PIPA that are critical to its effectiveness and should remain a strong part of the legislation. The first is the OIPC's order-making power, which puts the interests of those the *Act* is meant to protect – namely private citizens who share personal information with private sector entities – above those entities who would be conflicted about reporting data breaches at risk to their own reputations or bottom lines. At the federal level, PIPEDA has no such provisions yet in place, allowing private commercial actors excessive discretion to withhold notification with little to no consequence, in the event that their customers' personal information has been subject to a data breach.

The second positive element that the Alberta OIPC should maintain with respect to data breaches specifically is the consistent collection of statistics and related data. Good statistics regarding data breaches and breach notifications are limited in Canada, particularly given that reporting at all is still only mandatory in certain parts of the country, and federal data breach notification regulations have yet to come into effect.[7] As it is difficult to identify, let alone solve, problems or issues that are not tracked and measured, PIAC strongly recommends that the Alberta OIPC remain committed to its data collection and statistics-building work in the area of data breach notifications, in addition to other privacy protection matters.

Reject Attempts to Soften or "Harmonize" Alberta PIPA with PIPEDA

It is critical to the integrity of Canadians' privacy rights that the Alberta OIPC rejects attempts from either private sector parties or the federal government, or other provincial governments, to influence the PIPA review towards softening its provisions around data breach notifications or related issues. As Commissioner Jill Clayton said, Alberta is currently "a leader in Canada and internationally for its approach to private sector privacy."[8]

---

2 *Ibid.*, at pages 6, 32-34 (Table 1 and Graph 1).

3 John Lawford and Janet Lo, "Data Breaches: Worth Noticing?" Public Interest Advocacy Centre (December 2011), online: <https://www.piac.ca/wp-content/uploads/2014/11/data_breaches_worth_noticing_publication _version _final_final.pdf>, at page 88.

4 Phoenix Strategic Perspectives Inc., "Final Report: Canadian Businesses and Privacy-Related Issues: Prepared for the Office of the Privacy Commissioner of Canada" (December 2013), online: < https://www. priv. gc.ca /information/por-rop/2014/por_2013_12_e.pdf>, at page 24.

5 *Ibid*., at page 26.

6 EKOS Research Associates Inc., "Canadian Businesses and Privacy-Related Issues: Final Report" (March 2010), online: <http://www.ekospolitics.com/articles/03710.pdf>, at pages 30-31.

7 "While all other new provisions came into force upon the Act gaining Royal Assent, those dealing with breach reporting, notification and recordkeeping will be brought into force only after related regulations outlining specific requirements are developed and in place." Office of the Privacy Commissioner of Canada, The *Digital Privacy Act* (Fact Sheet), online: <https://www.priv.gc.ca/resource/fs-fi/02_05_d_63_s4_e.asp>.

8 Office of the Information and Privacy Commissioner of Alberta, "Presentation to the Standing Committee on Alberta's Economic Future," Speech (15 October 2015), online: < https://www.oipc.ab.ca/media/588470/ speech_pipa_review_oct2015.pdf>, at page 1.

This is because the new amendments to the federal *Personal Information Protection and Electronic Documents Act* as a result of Bill S-4 appear to be standard-setting but in PIAC's opinion clearly are inferior to Alberta's approach. As noted in PIAC's S-4 Senate appearance, the amended PIPEDA in new s. 10.1 *et seq.* yokes together customer notification with notification to the OPCC. This sets up a perverse incentive to NOT report breaches to the OPCC as such a report automatically and concomitantly requires reporting to all affected customers. The "all or nothing" approach of the federal legislation should not be emulated or "harmonized" with Alberta's clearly superior data breach notification scheme. PIAC also does not view the PIPEDA amendments requiring companies to secretly log (and produce for OPCC inspection upon request) data breaches that are not reported (to OPCC or customers) as likely to incentivize reporting adequately to counteract the main flaw described above. As we said to the Senate:

> True, companies must keep a record of all breaches to be available for inspection by the OPC – but why would the OPC target any particular company for such a check? The OPC hardly has the manpower to deal with the regular complaints it has, and simply will never be able to, for example, systematically pull such breach records for an industry over a 3-year or even a 1-year period. The breach records will remain, like the scarlet letter, a little corporate secret. Unfortunately for data breach victims, they will wear the loss of their data, while the OPC will be unaware of the breach and unable to audit or investigate.[9]

PIAC encourages the Alberta OIPC to continue upholding its commendable commitment to this issue. This is not only important for Albertans, but for people living across all other regions of the country, as other regulators or policymakers at both the provincial and federal levels have looked to Alberta's provisions as a model.

Room for Improvement

If there is one area for potential improvement of PIPA's data breach notification rules, that could be the area of empowering notified individuals to respond in the event of a data breach that has affected their personal information. While PIPA currently requires private organizations to notify impacted individuals of what steps the company has taken in response to the breach, there is little about informing those individuals of what steps they might personally take to mitigate impacts of a data breach. In PIAC's report on this issue, "Data Breaches: Worth Noticing?" (2011), focus group participants consulted for the report felt that "steps the individual can take to avoid or reduce the risk of harm or to further protect themselves ... would be one of the most valuable features of such a notice [of any breach]".[10] The Alberta OIPC may thus want to consider incorporating such a feature into the *Act*.

Conclusion

By now the various factors contributing to the rising importance of privacy and data protection are both legion and trite. In the case of Alberta's PIPA, maintaining a robust data breach notification regime becomes even more essential in light of trends that the Discussion Guide points out. These include increased sharing between the privacy sector, public sector, and health sector, and increased pressure from both governmental bodies and law enforcement on private sector entities to disclose increasing amounts of personal information without notice or consent. PIAC encourages the Alberta OIPC to continuing its strong stance in PIPA with respect to data breaches and notifications. Thank you for the opportunity to comment.

---

9 Remarks of the Public Interest Advocacy Centre, Before the Senate Standing Committee on Transport and Communications, in consideration of: Bill S-4, An Act to amend the Personal Information Protection and Electronic Documents Act and to make a consequential amendment to another Act, the "Digital Privacy Act", June 3, 2014.

10 Lawford and Lo, *supra* note 3 at pages 53-54.