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

May 31, 2016

Via email: ic.ised.breach-atteinte.isde.ic@canada.ca

Data Breach Consultations
Privacy and Data Protection Policy Directorate
Innovation, Science and Economic Development Canada
235 Queen Street
Ottawa, ON K1A 0H5

Re: PIPEDA Data Breach Notification and Reporting Regulations

The Canadian Bar Association Privacy and Access Law Section (the CBA Section) welcomes the opportunity to comment on Innovation, Science and Economic Development Canada's discussion paper on data breach notification and reporting regulations under the *Personal Information Protection and Electronic Documents Act* (PIPEDA).

The Canadian Bar Association is a national association representing approximately 36,000 jurists across Canada, including lawyers, notaries, law teachers and students, and its primary objectives include improvements in the law and the administration of justice. The Privacy and Access Law Section is comprised of lawyers with in-depth knowledge in the areas of privacy law and access to information. The CBA Section has made a number of previous submissions on PIPEDA.

General Comments

The CBA Section recognizes the importance of vigilance in monitoring and safeguarding personal information, and support the development of data breach notification and reporting regulations. We suggest that the regulations be consistent with the overall framework of PIPEDA, balancing individual privacy rights with the legitimate needs of businesses to collect, use and disclose personal information for reasonable purposes. In particular, we recommend a flexible, non-prescriptive approach to drafting the regulations, allowing assessment on a case-by-case basis and providing discretion to organizations to make appropriate decisions about their breaches. We also suggest that the Office of the Privacy Commissioner (OPC) is best placed to issue instructive guidance on many of the issues and questions identified in the discussion paper. Our comments are guided by our understanding of the overarching principle of balancing individual privacy rights and facilitation of commerce. In past submissions on PIPEDA, the CBA Section has advocated for this balanced approach.

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 | www.cba.org
Membership/Adhésion : memberservice@cba.org | **PD/DP :** pd@cba.org | **Sections :** cba.sections@cba.org | **General/Générale :** info@cba.org

Determining Real Risk of Significant Harm

In previous submissions on PIPEDA, the CBA Section addressed the issue of probability of access. In our 2005 submission,[1] we 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
- 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 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". The CBA Section believes it would be reasonable and practical for the level of encryption and the associated probability of access to be considered in assessing the real risk of significant harm. Of course, flexibility will be required in determining the level of encryption and associated risk. This should be left to the organization with the breach, since it arguably has the most relevant information to make such a determination.

Contents of Report to Commissioner

As stated in our 2008 submission,[2] the CBA Section encourages an approach to reporting where the report to the Commissioner is based on facts alone. We recommend not requiring notices and reports to include speculative assessments of the risk of harm. Among other issues, speculations are potentially prejudicial for the notifying or reporting organization, for example, where an individual may claim damages against the organization based on a privacy breach. The BC Information and Privacy Commissioner's Privacy Breach Reporting Form (November 2006) asks the organization to identify types of harm that may result from the breach. This type of reporting may actually discourage proactive reporting. A factually based form will encourage reporting.

Timing of Notification and Reporting

The CBA Section supports prompt notification to individuals where an organization has identified a "real risk of significant harm." However, we suggest that, instead of a specific timeframe, the timing of notification (and reporting) be flexible to accommodate particular considerations and circumstances of each breach. For example, it may be necessary to delay notification taking into consideration law enforcement and other investigations. Further, given the Commissioner's oversight role in this context, the time to report need not be short, allowing the organization time to complete its response to the breach and collect as many facts as possible to report. As is current practice today, however, organizations should be permitted to update reports as required.

Notification to Individuals and Other Organizations

The CBA Section recognizes the importance of providing meaningful notice to individuals of data breaches when appropriate. The regulations should avoid being overly prescriptive, however, in the form and manner of notifications. Organizations should have flexibility to determine whether direct or

---

1 Submission re: Preparing for the 2006 Review of the *Personal Information Protection and Electronic Documents Act* (Ottawa, CBA, August 2005)

2 Submission re: *Privacy Act* Reform (Ottawa, CBA, June 2008)

indirect notification is most suitable. The OPC could issue instructive guidelines to help organizations make this determination. The CBA Section also recommends that the regulations allow flexibility for organizations to assess other organizations to notify on a case-by-case basis. Again, the OPC is best placed to issue guidance on this issue.

Record-Keeping Requirements

The CBA Section recommends providing clear record-keeping requirements without being overly prescriptive. Absent draft regulations or instructive OPC guidelines, it is difficult to know what constitutes an acceptable record and, similarly, an acceptable record-keeping practice. The issues on keeping records are particularly problematic as not keeping adequate records constitutes an offence under section 28 of PIPEDA. The OPC is well suited to offer guidelines on who in an organization may be best placed to act as record keepers, as well as details on record retention periods, the manner in which records must be designed and maintained and the level of detail required in the report. The CBA Section suggests that the record-keeping requirements be flexible and reasonable, without becoming an administrative burden for organizations.

Conclusion

The CBA Section appreciates the opportunity to offer input on PIPEDA's data breach notification and reporting regulations. We support establishing these regulations and believe an effective regulatory regime in line with our recommendations will further entrench an organization's obligations to safeguard personal information and strike an appropriate balance between individual privacy rights and the facilitation of commerce.

Yours truly,

(original letter signed by Gillian Carter for Laura W. Davison)

Laura W. Davison
Chair, CBA Privacy and Access Law Section