

reforming PIPEDA with stronger enforcement powers, mandatory breach notification and accountability obligations

The Privacy Commissioner of Canada Jennifer Stoddart has released her report entitled "*The Case for Reforming the Personal Information Protection and Electronic Documents Act*" earlier today outlining her proposals for modernizing Canada's private-sector privacy legislation to ensure that it is able to meet the new challenges of the digital age.

As a matter of fact, the environment in which personal information is collected, used and disclosed has undergone a dramatic reshaping since the *Personal Information Protection and Electronic Documents Act* (PIPEDA) was initially passed. We now live in the era of "big data" and with those changes have come risks that individuals' information may be used in ways that may be intrusive, or that personal information may not be protected by sufficient or adequate security measures.

The Office of the Privacy Commissioner of Canada now has more than a decade of practical, hands-on experience in investigating privacy complaints, conducting audits, and monitoring security breaches brought to their attention or through media reports. The report explains how a stronger enforcement regime to ensure that Canadians' personal information is appropriately protected in a complex, globally connected environment is now becoming a necessity.

It is recommended that the following changes be made to PIPEDA:

- • **Provide for stronger enforcement powers.** The report states "The days of soft recommendations with few consequences for non-compliance are no longer effective in a rapidly changing environment where privacy risks are on the rise." These new powers could include statutory damages (administered by the Federal Court), giving the Commissioner the power to make orders, affording the Commissioner with the power to impose administrative monetary penalties or a combination of the above.
- • **Mandatory breach notification and reporting.** Under the proposed reform, security breaches would have to be reported to the Commissioner and affected individuals would have to be notified in order to ensure that appropriate mitigating measures can be taken in a timely manner. These types of changes would be in line with Alberta's PIPA, Alberta being the only jurisdiction in Canada with a comprehensive mandatory data breach requirement covering the private sector. The [OIPC's Report](#) on two years of mandatory breach reporting in Alberta released in June 2012 confirms how the majority of breaches usually involve human error, such as misdirected emails, faxes, stolen or lost unencrypted electronic devices and improper record and electronic media destruction. These types of security breaches have also been recently reported in the news with the Human Resources and Skills Development Canada (HRSDC) who lost an unencrypted hard drive containing the personal information of 583,000 individuals who had a student loan and contact information of 250 HRSDC employees (January 2013), and the Investment Industry Regulatory Organization (IIROC) who lost an unencrypted laptop containing financial information of 52 000 brokerage firm clients (April 2013). Interestingly, the Office of the Privacy Commissioner of Canada's most recent [business survey](#) found that companies in Alberta were the most likely to deliver privacy training to their employees compared to other provinces. This is a clear indicator that these types of mandatory breach notification provisions will

create the incentive for organizations to invest in preventive data protection measures.

- • **Obligation to report disclosures made to law enforcement.** Another proposed change relate to the obligation for organizations to publicly report the number of disclosures made to law enforcement under paragraph 7(3)(c.1) of PIPEDA. Since these disclosure are made without the knowledge or consent of affected individuals and without judicial warrant, this requirement will shed light on the frequency and use of this extraordinary exception.
- • **Obligation to demonstrate accountability.** A last proposed change relate to modifying the accountability principle in Schedule 1 of PIPEDA in order to include a requirement for organizations to demonstrate accountability upon request, to incorporate the concept of "enforceable agreements", and to make certain accountability provisions subject to review by the Federal Court of Canada.

The Privacy Commissioner of Canada rightfully believes that such measures will address current and future privacy challenges, improve Canadians' trust in the digital economy, reinforce Canadian innovation and growth and ensure that Canada remains a country with an appropriate, up-to-date and balanced privacy framework.

by [Éloïse Gratton](#)

For more information on this topic, please contact:

Montréal

[Éloïse Gratton](#)

514.987.5093

eloise.gratton@mcmillan.ca

a cautionary note

The foregoing provides only an overview and does not constitute legal advice. Readers are cautioned against making any decisions based on this material alone. Rather, specific legal advice should be obtained.

© McMillan LLP 2013