OSLER

Privacy a primary concern in 2017

DECEMBER 13, 2017 5 MIN READ

Related Expertise

- Privacy and Data Management

Authors: Adam Kardash, Joanna Fine, John Salloum, Christopher Naudie, Evan Thomas

Sophisticated cybersecurity threats, high-profile data incidents, and an explosion in the volume of data analytics initiatives have resulted in privacy issues being top of mind for organizations across all sectors. Moreover, in 2017, there were several key legal and regulatory developments in the Canadian privacy and data arena, most notably relating to statutory security breach notification regimes, Canada's Anti-Spam Legislation (CASL), and data governance.

Security breach notification

The *Personal Information Protection and Electronic Documents Act* (or PIPEDA) – Canada's federal private sector privacy law – has a new security incident reporting and notification regime, which will come into force after regulations are finalized.

The new regime features a unique, three-pronged notification requirement. When an organization suffers a breach of security safeguards that gives rise to a "real risk of significant harm" in the circumstances, the organization must (i) report the incident to the Office of the Privacy Commissioner of Canada (the OPC); (ii) notify affected individuals; and (iii) notify any other third parties that are in a position to mitigate the risk of harm to affected individuals.

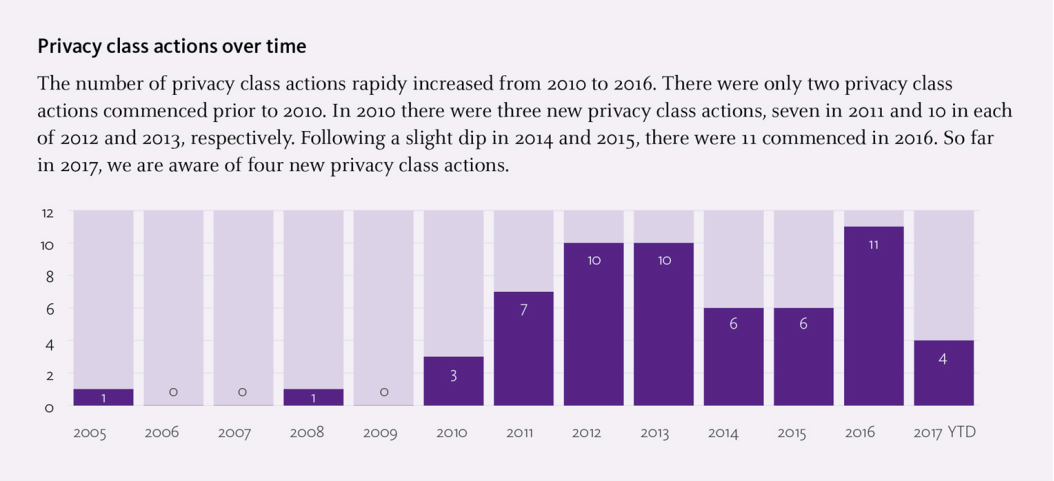
Critically, PIPEDA's new security breach notification regime also imposes a record-keeping requirement, under which organizations must maintain a record of all of their data breaches. Organizations are obligated under the statute to make these records available to the OPC upon request.

Draft security breach regulations were released this past September. It is expected that they will be finalized in 2018 and come into force thereafter, following a brief transition period.

We expect this notification regime to have a significant effect on the Canadian data arena. Based on client experience after U.S. states implemented their security breach notification regimes several years ago, after the *Personal Information Protection Act* (Alberta) was amended to include an incident reporting rule, and after notification rules were introduced in various provincial health privacy statutes (including enhanced rules in Ontario's health privacy legislation that came into force this year), we are expecting PIPEDA's new reporting and notification regime to have the following consequences:

- More transparency about and reporting of data security incidents within organizations, and more general awareness about the increasing volume, breadth, and sophistication of security threats.

- More notifications sent to affected individuals and other organizations about security incidents.
- More media coverage, or at least a spike in media reports, and heightened public awareness about information security safeguarding practices (or a perceived lack thereof).
- More investigations, posted decisions, and regulatory queries by privacy regulatory authorities, leading to a continuing increase in the sophistication of privacy regulatory authorities, which will, in turn, raise regulatory expectations.
- Increased class action litigation risk.



- More concern about and attention to the enhanced legal and reputational risks at the senior management and board level.
- More proactive efforts by organizations to address personal information security concerns, initially focusing, in particular, on
  - developing and/or enhancing and ensuring the appropriate implementation of security incident readiness plans and protocols; and
  - intensified scrutiny of third-party vendors who have custody of the data of organizations, including enhanced vendor management practices, such as increased pre-contractual due diligence, more robust contractual obligations on vendors to safeguard data, more attention on appropriate risk allocation, and a focus on post-contractual compliance monitoring.
- And, overall, increased costs to organizations due to all of these factors.

Canada's Anti-Spam Legislation

CASL is perhaps the most stringent anti-spam legislation in the world. The legislation imposes strict and prescriptive consent, notice, and other requirements relating to the sending of commercial electronic messages and the installation of computer programs.

To date, the Canadian Radio-television and Telecommunications Commission (CRTC) – the primary body responsible for enforcing CASL – has received over 1 million complaints involving alleged violations of CASL. The penalties for non-compliance are potentially severe: organizations can be subject to administrative penalties of up to $10 million and a private right of action for damages of up to $200 per commercial email (or other type of electronic message) sent in contravention of the legislation, up to a maximum of $1 million for each day the contravention occurred.

The private right of action was originally scheduled to come into force on July 1, 2017. However, in a significant development in June of 2017, the Canadian federal government announced that it was suspending the coming into force of these provisions, noting that a parliamentary committee would be asked to review CASL.

The House of Commons Standing Committee on Industry, Science and Technology commenced the parliamentary review this past September and proceeded rapidly with its work. By early November, the Committee had heard from dozens of witnesses and received dozens of written briefs, the vast majority of which advocated for significant amendments to CASL. The federal government's response to the report of this parliamentary committee is expected in 2018.

In the meantime, companies still face potential CRTC enforcement for violations of CASL. The CRTC concluded several investigations in 2017 and has multiple other investigations in progress.

The data governance focus

Data is now regarded as a "business critical" asset of many organizations, and significant corporate resources in analytics are being dedicated to leverage the benefits of the vast (and rapidly growing) amount of information in their custody and control.

Companies in all sectors are coming to grips with the nuanced privacy, legal, ethical, and reputational risks arising in the course of their analytics (i.e., "big data" initiatives). In a major trend aimed at identifying and mitigating these risks, more organizations have been developing or enhancing robust data governance frameworks, that incorporate privacy programs, information security governance and enterprise risk processes.

In 2017, Canadian privacy regulatory authorities also turned their attention more to organizations' privacy programs, data governance and "demonstrable accountability." In regulatory decisions and a number of public statements, privacy regulatory authorities more pointedly emphasized the need for organizations to demonstrate the effectiveness of the policies, practices, and procedures governing their personal information practices.

Moving into 2018, we are expecting that "demonstrable accountability" will remain a central focus of Canadian privacy regulatory authorities. Canadian organizations should ensure that they are in a position to demonstrate that they have up-to-date and appropriately robust data governance frameworks in place.