OSLER

Data breaches and law reform capture international attention in 2019

DECEMBER 13, 2019 7 MIN READ

Related Expertise

- Privacy and Data Management

Authors: Adam Kardash, Patricia Kosseim

Organizations faced a continuing crescendo of complex privacy and data governance issues through 2019, making it another highly eventful year in privacy law.

Mandatory breach notification after one year

November 2019 marked the first full year of mandatory breach notification under the federal *Personal Information Protection and Electronic Documents Act* (PIPEDA).

The privacy regulator blogged about a 600% increase in data breaches reported to the Office of the Privacy Commissioner of Canada (OPC) over the past twelve months. According to the OPC, more than 28 million Canadians were affected by these reported data breaches, 58% of which involved unauthorized access and a quarter of which involved social engineering attacks.

These statistics certainly correspond with a trend we saw unfolding with our clients. Many of Canada's largest corporations reached out for assistance in responding to harrowing experiences with ransomware and data extortion attempts that threatened to undermine their reputations, not to mention their operations. Many other organizations reached out proactively to seek assistance in developing agile breach incident response plans so they could be well prepared in advance if and when they fall prey to similar attacks.

Data transfers to third parties

The kerfuffle surrounding the rules applicable to data transfers to third parties for processing finally settled down after a tumultuous year. This upheaval was triggered by a change in OPC's longstanding policy position when it found, in the context of an investigation into a data breach matter, that Equifax Canada should have obtained consent from its customers prior to sending their data to its U.S. parent company for the purposes of processing their requests for certain direct-to-consumer products.

The OPC subsequently launched consultations to seek input from a broader range of stakeholders on whether this consent requirement should be generalizable to others. The OPC received 87 submissions from stakeholders (see Osler's AccessPrivacy submission here). The vast majority took the view that the current law does not require consent for transfers for processing, and that imposing such a requirement would create "enormous challenges" for organizations' business processes.

Clearly influenced by all the compelling counterarguments it received, the OPC decided to

adopt a "flexible, common-sense and pragmatic approach" and restored its earlier 2009 Guidelines for processing personal data across borders that did not require consent for processing. Maintaining its view that existing privacy protections are "clearly insufficient," the OPC vowed to make recommendations to strengthen these protections in the context of PIPEDA reform.

PIPEDA reform

On the subject of PIPEDA reform, stronger enforcement, enhanced accountability and possible consent exceptions were among the topics garnering much attention. Together with the unveiling of Canada's Digital Charter, Innovation, Science and Economic Development (as it was then called) released its white paper "Strengthening privacy for the digital age" (PIPEDA White Paper) containing a number of reform proposals for PIPEDA. In parallel, Justice Canada released another series of discussion papers proposing a significant "rethink" of Canada's public sector privacy law as well.

However, in the weeks leading up to the 2019 federal election in October, all consultations were suspended out of respect for the caretaker convention. Interestingly, the 2019 federal election itself further elevated the pressing nature of privacy and data security issues in the minds of Canadians. For the first time, the protection of Canadians' personal information made its way explicitly into the electoral platforms of all the major parties.

A unanimous resolution of Canada's federal, provincial and territorial commissioners calling for privacy and access law reform is likely to reignite the sense of urgency under the new minority government as this file competes for attention among many other priorities. In the Speech from the Throne 2019, the Government vows to advance "the development and ethical use of artificial intelligence" and to review current rules "to ensure fairness for all in the new digital space". What compromises will have to be made, and with which other political parties, remains to be seen in the months ahead. Early statements by the Minister of Innovation, Science and Industry indicate a firm commitment to press forward on privacy law reform. Should a legislative proposal indeed be tabled in this next Parliamentary session, stronger enforcement will almost inevitably form part of the package.

Increased international enforcement

Ramped-up enforcement was certainly a major theme internationally as well. International data protection authorities made major commitments to collaborate more closely on enforcement action and to facilitate cooperation with regulatory authorities in related fields of competition and consumer protection to ensure more consistent standards of data protection in the digital economy.

The International Conference of Data Protection and Privacy Commissioners (ICDPPC) met in Tirana, Albania in October 2019. The ICDPPC adopted a number of international resolutions reflecting their converging perspectives on some of the most pressing data protection issues of the day. They called on relevant stakeholders to address the need for appropriate safeguards to reduce the role of human error in data breaches and urged social media providers to take steps to stop the dissemination of extremist online content using their platforms, while continuing to protect freedom of expression.

Most interestingly, an OPC-sponsored resolution urged governments around the world to reaffirm their strong commitment to privacy as a fundamental human right, vital to the protection of other democratic rights. Businesses were urged to show demonstrable accountability by actively respecting privacy and other human rights as a key aspect of legal

compliance, corporate social responsibility and an ethical business approach.

The EU General Data Protection Regulation

Continuing on the international theme, the EU *General Data Protection Regulation* (GDPR) settled into its second year of existence. Many global companies refined their privacy compliance frameworks, while EU Data Protection Authorities eased more comfortably into their enforcement role by unleashing hefty fines against those companies that didn't.

California's new privacy measures

All the hype around GDPR gave way this year to the *California Consumer Protection Act* (CCPA). Scheduled to come into effect January 1, 2020, the CCPA overtook much of the global attention this year not only because of the law itself, but also as a result of the strong influence it is having on many other U.S. states that are following California's lead and adopting and/or proposing similar state laws. This has prompted a strong lobby by some of the world's largest Internet giants for a more consistent, unified, U.S. federal privacy law.

New self-regulatory initiatives

Finally, this past year saw a growing number of stakeholders taking proactive steps themselves in the absence of law reform to find more innovative ways of protecting data. Some have taken up the invitation by regulatory authorities to participate in regulatory sandboxes, while others have developed ethical frameworks for the use of artificial intelligence and innovative privacy enhancing technologies.

Among these was the official launch of the Canadian Anonymization Network (CANON), a registered not-for-profit corporation co-founded by AccessPrivacy and several other leading organizations across public, private and health sectors. CANON supports the common mission to promote anonymization as a privacy-respectful means of innovating with data for socially- and economically-beneficial purposes.

As one of its first deliverables, CANON responded to ISED's request for comments on the deidentification issues and opportunities raised in its PIPEDA White Paper. In its Submission, CANON called for consistency of standards and definitions. CANON also advocated for a balanced legislative framework which: recognizes the contextual aspects of anonymization; adopts a more risk-based approach; clarifies the role of consent; and allows room for industry codes of practice that enable flexible, innovative and beneficial uses of data, while reasonably protecting against foreseeable privacy risks.

If privacy was in the public eye in 2019, it promises to be an even more glaring issue in 2020 as Canada looks to modernize its privacy laws while the rest of the world ratchets up the stakes.