OSLER

Privacy stakes higher than ever in 2018 for regulators, businesses and citizen

DECEMBER 18, 2018 6 MIN READ

Related Expertise

- Privacy and Data Management

Authors: Adam Kardash, Patricia Kosseim

Major data breaches the world over have caught the attention of boards of directors. Boards are becoming increasingly seized with these issues and starting to ask more scrutinizing questions of senior management about the privacy and security posture of their organizations. Regulators have been fortified in their data protection mission and, together with consumer protection, competition and human rights regulators, are increasingly co-ordinating their efforts to combat global internet giants and the privacy risks posed by new and emerging business models. Parliamentarians are likewise concerned about the efficacy of Canada's laws in responding to growing cyber risks that are threatening privacy, critical infrastructure and democracy itself. Committee after committee, report after report, and recommendation after recommendation have called for Canada's privacy laws to be strengthened and the Federal Privacy Commissioner to be granted more powers and resources. And consumers and citizens are becoming increasingly irate with media reports about what is being done with their personal data behind the scenes. They are starting to push back by signing petitions, lodging complaints and voting with their feet.

Privacy and security stakes shot up for everyone in 2018, across sectors, industries and jurisdictions, with data breaches, EU's GDPR and digital ethics taking centre stage.

New mandatory breach notification regime is now in force

After years in the making, the coming into force of a new mandatory breach notification regime under PIPEDA, Canada's federal private sector privacy law and accompanying regulations, occurred in November 2018. These changes introduced legal obligations for companies to report data breaches above a certain threshold to the Privacy Commissioner. To help mitigate any further risk of harm, reports must also be made to affected individuals and to relevant organizations like law enforcement and credit monitoring companies. Companies must now also keep records of all privacy breaches, regardless of materiality, and must be ready to produce such records anytime the regulator comes knocking.

In support of these new requirements, PIPEDA was further amended to introduce potentially hefty fines in cases of non-compliance. Material fines and penalties should be a major incentive for corporations to prioritize the company's breach incident readiness and response plan —something Osler has helped many businesses develop and/or strengthen throughout this past year.

The EU's General Data Protection Regulation has global impact

No privacy review of 2018 would be complete without mentioning the coming into force of the European Union's (EU) General Data Protection Regulation (GDPR) in May of this year. The GDPR has had an overwhelming impact all over the world, well beyond the EU's borders. Many global companies have had to "up their privacy game" to meet the more stringent EU requirements and have done so across all their related companies and subsidiaries around the world for purposes of standardization and consistency. Even Canadian companies with no establishments in the EU have had to comply with GDPR requirements to the extent they are caught by the extended reach of its extraterritorial scope provisions. Specifically, the GDPR applies where companies offer goods or services to EU data subjects, or monitor their behaviour in the EU, including through online behavioural advertising.

Moreover, legislators around the world, including in Canada, have had to re-examine the state of their privacy and national security laws if they wish to obtain (or in Canada's case, preserve) their adequacy status under the GDPR. Preservation of adequacy status is important in order to continue transferring personal data with relative ease across the Atlantic as part of Canada's commercial trade with Europe.

U.S. state laws could motivate federal initiatives

The situation south of the border has likewise seen some interesting twists and turns this year. After years, if not decades, of "all talk no action," lawmakers hastily adopted the *California Consumer Privacy Act* (CCPA) in a strategic and last-ditch effort to stave off what would have been an even stricter privacy regime slated for a state-wide ballot initiative.

Signed into law on September 23, 2018, the CCPA is expected to come into force on July 1, 2020, pending substantive changes that have yet to be considered in the New Year. Although it is still a moving target, the CCPA is having the indirect effect of leveraging a strong lobby for the adoption of a U.S. federal privacy law. Such a measure is viewed as a way of curbing the appetite of many individual states to follow in California's footsteps with their own laws —which risks creating a tapestry of inconsistent standards across the U.S. and wreaking havoc for businesses.

It is telling that the CEO of Apple, Senior VP of Google and Global CPO of Facebook, when asked at the 40th International Data Protection and Privacy Commissioners' Conference in October of this year whether they would support the adoption of a U.S. federal privacy law, all responded with a resounding and unequivocal "yes."

Digital ethics gains resonance with advent of artificial intelligence

The entire theme of this year's 40th International Data Protection and Privacy Commissioners' Conference was digital ethics. Regulators around the world are beginning to explore ways of supplementing privacy laws with ethical governance frameworks to address the broader societal and moral questions arising from the use of artificial intelligence (AI) and machine learning. International data protection authorities unanimously adopted a Declaration on Ethics and Data Protection in Artificial Intelligence. The Declaration is comprised of a series of governing principles including fairness, algorithmic transparency, non-discrimination, demonstrable governance processes, the need for independent ethics committees and an overall ethics by design approach – all of which businesses can expect to hear more about in the course of future regulatory action.

Although this may sound like remote Brussels talk, it is particularly germane for Canada as it positions itself strategically to become a world leader in AI and machine learning. At the time of writing, the Canadian government had just announced significant new investments in AI in the form of major funding for six companies engaged in AI development.

Conclusion

A number of regulatory initiatives took effect in 2018. At the same time, the accelerated pace of technological innovation, including AI, raises new and complex privacy risks. Major initiatives like Toronto's Sidewalk Labs, the "race" for road-safe connected and automated vehicles, and our continuing competitive edge in the area of personalized pharmaceuticals all stand to deliver tremendous social and economic benefits to Canadians, so long as we can address the privacy risks and ethical concerns they give rise to and build in the protections needed to ensure their respectful and responsible deployment.