Canada’s New Privacy Regime In Alberta

While most of us will remember 2020 as the year of the pandemic, privacy nerds (they do exist) will also remember a year of large-scale federal and provincial privacy reforms that will carry into 2021 and beyond.

The Government of Canada tabled Bill C-11, which would repeal Part 1 of the outdated *Personal Information Protection and Electronic Documents Act* (PIPEDA) and replace it with a modernized legislative regime governing the collection, use, and disclosure of personal information for commercial activity in Canada. The *Consumer Privacy Protection Act* (CPPA), the centerpiece of Bill C-11, continues to advance the principles of protecting individuals’ personal information while recognizing organizations’ need to collect, use or disclose personal information in the course of commercial activities. Bill C-11 would also establish a Personal Information and Data Protection Tribunal to hear appeals of certain decisions made by the Privacy Commissioner under the CPPA, and to impose penalties for specific violations.

Expanded rights and modern consent rules

Under the CPPA, organizations must implement a “privacy management program” (which includes the organization’s privacy policies and procedures) and may collect, use or disclose personal information only for purposes that a reasonable person would consider appropriate in the circumstances. An organization must determine and record that purpose at, or before the time of the collection. Individuals may ask organizations how their personal information is being used and to whom it has been disclosed.

Many hallmark requirements for express consent to collect, use, and disclose personal information are carried over from PIPEDA to the CPPA. The CPPA attempts to clarify circumstances where consent may not be required, including for certain business activities. While implied consent can still be valid, organizations must consider the “reasonable expectations of the individual and sensitivity of the information”.

The CPPA proposes to introduce provisions that strengthen an individual’s ability to control their personal information. These provisions include:

- The right to request an organization to dispose of personal information collected from the individual. This requirement extends to third-party service providers that may have received personal information from the

organization.
- A private right of action for damages against an organization after the Privacy Commissioner or the Data Protection Tribunal makes a finding that it contravened the CPPA, or if the organization is convicted of certain offences.
- Additional rules relating to the de-identification of data and how de-identified data may be used by organizations.

New Commissioner powers, enforcement, and the Data Protection Tribunal

Bill C-11 proposes a significant overhaul to the Commissioner's oversight and enforcement powers. The CPPA would give the Commissioner broad order-making powers, including the ability to order a company to stop collecting data or cease using personal information. Further, the Commissioner can conduct inquiries after investigating a complaint. Following an inquiry, the Commissioner may recommend that a penalty be imposed on the organization by the Tribunal. Maximum penalties are significant and not currently seen in PIPEDA. Administrative monetary penalties are up to 3% of global revenue or $10 million for non-complaint organizations in the financial year prior to the penalty. Organizations prosecuted for more egregious conduct, including knowingly contravening breach reporting and notification requirements, failing to retain personal information subject to an access request, and obstructing the Commissioner during the investigation and inquiry processes are subject to a maximum fine of 5% of global revenue or $25 million.

The Tribunal would hear appeals from findings, orders, or decisions of the Commissioner. Further, the Tribunal is tasked with assessing and imposing fines for penalties, as the Commissioner may only make recommendations.

Stimulus for change

The federal changes introduced through Bill C-11 are part of the cascading effect of privacy reforms seen in other parts of the world, including the *General Data Protection Regulation* (GDPR) that came into force in 2018 in the European Union. Advocates of a strong privacy rights-based approach may be left wanting more, but Bill C-11 is the most significant set of federal privacy reforms in over a decade. The new privacy legislation also arrives at a time of increasing public awareness of privacy issues arising from a year of heavy technological reliance. It's a new environment in which organizations will have to pay specific attention to the protection of individuals' personal information.

Impact on Alberta

Where does this take provinces like Alberta that have long prided themselves on having progressive privacy legislative regimes? Alberta's *Personal Information Protection Act* (PIPA) is deemed "substantially similar" to PIPEDA. An organization's compliance with PIPA usually meant that they were complying with PIPEDA. With the Bill C-11 forging ahead, PIPA risks being left behind. Certain structural changes, like the introduction of a tribunal, were not part of reform recommendations made by the Alberta Information and Privacy Commissioner. Some may question whether it was a necessary addition at the federal level. However, provinces like Alberta will undoubtedly look at

strengthening their own legislation and may look to incorporate principles like the right to be forgotten and data-portability. Failing to provide similar protections may risk a loss of substantial similarity between provincial and federal legislation, and the broader application of the federal counterpart in Alberta.

In carrying out its powers and duties under the CPPA, the Commissioner must take into account the size and revenue of organizations, the volume and sensitivity of the personal information under their control and matters of general public interest. Regardless of size or sophistication, all organizations will need to take precautions. No longer can privacy and data management issues be isolated and delegated solely to the responsibilities of a privacy officer or information technology professional. These are compliance issues that the organization as a whole must address. Failing to do so will increase the risk of not only fines, but significant reputational harm and loss of client goodwill.

by Marc Yu and Lyndon Bolanac
Field LLP