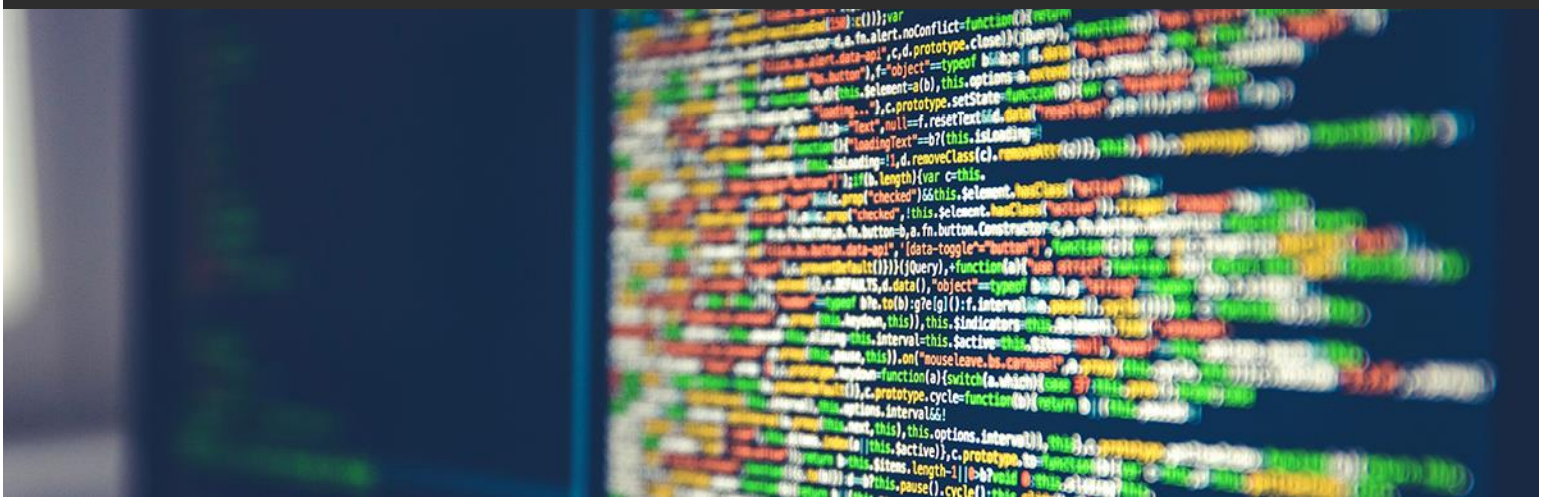
GT GreenbergTraurig

Alert | Data, Privacy & Cybersecurity



November 2020

Canada Proposes Federal Privacy Law Overhaul – Key Takeaways

On Nov. 17, 2020, the Canadian government introduced the Digital Charter Implementation Act, 2020 (DCIA, or Bill C-11), a much-anticipated bill aimed at overhauling the country's comprehensive private sector data privacy legal regime. As introduced by Minister of Innovation, Science and Economic Development Navdeep Bains, the DCIA would establish a new privacy law for the private sector – the Consumer Privacy Protection Act (CPPA).

If passed in its current form, the CPPA would usher in sweeping changes to the Canadian privacy landscape, from enhanced individual rights, to data mobility, to far more punitive enforcement powers for the federal privacy regulator. The law would apply to personal information that is "collected, used, or disclosed interprovincially or internationally by an organization."

The proposed update to Canada's privacy laws comes as other countries that have received an adequacy determination from the European Commission, as Canada did in 2002, are reevaluating their domestic data protection legislation in light of the Court of Justice for the European Union's *Schrems II* ruling in July 2020, which invalidated the EU-U.S. Privacy Shield Framework, signaling a much tougher stance on what Europe considers insufficient privacy protections in its trading partners.

Background

The Canadian government has signaled for over a year that it would seek to strengthen and modernize the federal Personal Information Protection and Electronic Documents Act (PIPEDA), an element of the country's Digital Charter strategy. In late 2019, Prime Minister Justin Trudeau instructed Minister Bains "to establish a new set of online rights, including: data portability; the ability to withdraw, remove and erase basic personal data from a platform; the knowledge of how personal data is being used, including with a national advertising registry and the ability to withdraw consent for the sharing or sale of data[,]" and more.

Global technology changes over the last two decades and recent privacy rights developments such as the EU's General Data Protection Regulation (GDPR) or the California Consumer Privacy Act (CCPA) in the United States appear to be motivating factors behind Canada's proposed updates.

Creation of Privacy Tribunal and Large Fines

Federal Enforcement Power and Steep Fines

A glaring shortcoming of Canada's current federal privacy law, PIPEDA, is the fact that the Office of the Privacy Commissioner (OPC) serves as more of an ombudsman. That is, while the Privacy Commissioner can investigate complaints and enter compliance agreements with alleged violators, it has no power to levy fines or penalties for PIPEDA violations. This can be contrasted with regulators under the GDPR, CCPA, Brazil's LGPD, and other privacy legal frameworks around the world.

The OPC also lacks even general enforcement authority, as its powers "focus[] on resolving complaints through negotiation and persuasion, using mediation and conciliation if appropriate," and "if voluntary co-operation is not forthcoming, the Commissioner has the power to summon witnesses, administer oaths and compel the production of evidence."

The CPPA would give the OPC coercive power for the first time, empowering the federal privacy commissioner to order a company to cease processing activities, and to impose fines up to C$25,000,000 or 5% of the organization's global revenue for certain offenses, or in the case of less serious offences, up to C$20,000,000 or 4% of global revenue.

Creation of a New Privacy 'Tribunal'

Part 2 of the DCIA also creates a new enforcement agency called the "Personal Information and Data Protection Tribunal" (the Tribunal), which would hear any appeals from orders from the OPC. The Tribunal's orders would be considered final (with some exceptions for possible judicial review by higher courts pursuant to Canadian law). At least one member of the Tribunal, to be composed of three to six members, must be an expert in privacy law.

Updates for Individuals

Enhanced Individual Rights

The CPPA proposal does not exist in a vacuum, as Canada's PIPEDA framework, which came into force in stages between 2001 and 2004, already requires businesses to afford certain privacy protections to Canadians. As the OPC notes in its summary of PIPEDA, "Organizations covered by PIPEDA must generally obtain an individual's consent when they collect, use or disclose that individual's personal

information. People have the right to access their personal information held by an organization. They also have the right to challenge its accuracy."

The CPPA advances data portability/mobility rights (i.e., the ability for an individual to direct an organization to seamlessly transfer data to another organization); as well as deletion rights, including in relation to personal information (PI) on social media platforms; and increased ease of withdrawing consent to use an individual's information.

Algorithmic Transparency

Borrowing from the EU's GDPR, the CPPA requires businesses to transparently describe to individuals any use of an automated decision system – such as algorithms and artificial intelligence – to make predictions, recommendations, or decisions about individuals that could have a significant impact on them. Individuals also have the right to request an explanation as to how information about them was obtained as well as how any prediction, recommendation or decision was made by an automated decision-making system.

Private Right of Action

Notably, the CPPA also provides a private right of action for individuals affected by an organization's violation of that law by act or omission. The CPPA provides that affected individuals can sue for "damages for loss or injury" if the OPC has rendered a final finding that the organization contravened the CPPA. A two-year statute of limitations exists from the date of the OPC's finding of a violation or award of damages, and a claim may be brought either in the Federal Court of Canada or in the superior court of a Canadian province.

Updates for Businesses

Business Interests-Based Exceptions to the Consent Requirement

The CPPA recognizes that a business may collect or use an individual's PI without their knowledge or consent if the collection is made for certain business activities, provided a reasonable person would expect such a collection or use for that activity, and the PI is not used for the purpose of influencing the individual's behavior or decisions.

Acceptable activities include: when necessary to provide or deliver a requested product or service; when carried out to prevent or reduce commercial risk; when necessary for an organization's information, system or network security; when necessary for the safety of a product or service; when obtaining consent is impractical due to the absence of a direct relationship with the individual; and for any other activity prescribed by future regulations.

Use of De-Identified Data Without Consent

The bill also establishes that businesses may use de-identified PI without an individual's consent under certain circumstances – such as for internal research and development or in the context of a prospective business transaction. It requires that a business ensure that any technical and administrative measures applied to the information are "proportionate to the purpose for which the information is de-identified and the sensitivity of the [PI]." Further, organizations are prohibited from using de-identified information in combination with other data that would re-identify an individual.

Privacy Management Program Requirement

Taking into account the volume and sensitivity of the PI under its control, the CPPA requires that every organization implement a "privacy management program" comprising the business's policies, practices and procedures put in place to fulfill its obligations under the law. This includes in relation to the protection of PI; the receipt and handling of individual rights requests; staff training; and supporting policies and documentation that explains the implementation the law across the organization. Upon request, an organization must provide the OPC with access to such policies, practices and procedures.

Service Providers

The bill also explicitly addresses service providers, defined in the text as any organization which "provides services for or on behalf of another organization to assist the organization in fulfilling its purposes," and which includes subsidiary or affiliate corporations and contractors. If an organization transfers PI to a service provider, the organization must ensure – "by contract or otherwise" – that the service provider provides substantially the same protection of the PI that the organization is required to by the CPPA. The bill would exempt service providers from most of the CPPA's obligations in relation to the PI transferred to the service provider by an organization – other than security and data breach notification requirements – unless the service provider collects, uses, or discloses such information for any purpose other than that for which the PI was transferred.

Consent in Relation to Service Providers

Addressing a matter at the heart of the OPC's 2019 investigation of Equifax Canada, in which the OPC found that meaningful consent was not obtained from Canadian individuals before disclosing their PI to Equifax Inc. in the U.S. for processing, the CPPA clarifies that an organization may transfer PI to a service provider without an individual's knowledge or consent.

Recognition of Certification Systems and Codes of Practice

To help organizations understand their obligations under the CPPA and demonstrate compliance, the legislation would allow organizations to ask the OPC to approve codes of practice and certification systems that set out rules for how the CPPA applies in certain activities, sectors or business models.

Conclusion

The DCIA or "Bill C-11" has only just been introduced, and currently there is no timeline for when a finished bill might make its way through both the House of Commons and the Senate, and receive royal assent to finally become a law. Before that can happen, it can be expected that the bill will receive multiple readings in both houses, as well as review in multiple committees and further revision and debate. There is also currently no timeline for future implementation or enforcement of these provisions, as by the bill's own terms the finalized law would "come into force on a day to be fixed by order of the Governor in Council" in Canada.

** Greenberg Traurig is not licensed to practice law in Canada and does not advise on Canada law. Specific Canada law questions and Canada legal compliance issues will be referred to lawyers licensed to practice law in Canada.*

GT GreenbergTraurig

Authors

This GT Alert was prepared by:

- Darren Abernethy | +1 415.655.1261 | abernethyd@gtlaw.com
- Gretchen A. Ramos | +1 415.655.1319 | ramosg@gtlaw.com
- Michael C. Hoosier | +1 415.655.1276 | hoosierm@gtlaw.com

Albany. Amsterdam. Atlanta. Austin. Boston. Chicago. Dallas. Delaware. Denver. Fort Lauderdale. Germany.¬ Houston. Las Vegas. London.* Los Angeles. Mexico City.+ Miami. Milan.» Minneapolis. New Jersey. New York. Northern Virginia. Orange County. Orlando. Philadelphia. Phoenix. Sacramento. Salt Lake City. San Francisco. Seoul.∞ Shanghai. Silicon Valley. Tallahassee. Tampa. Tel Aviv.^ Tokyo.¤ Warsaw.~ Washington, D.C.. West Palm Beach. Westchester County.