CAOB
CAROL ANNE O'BRIEN
BARRISTER & SOLICITOR

OFFICE 416·640·7270 EMAIL caob@caobrienlaw.com MOBILE 416·399·6270 WEB caobrienlaw.com
151 Yonge Street, Suite 1500 Toronto, ON M5C 2W7

November, 2022

Privacy Law Update, Bill C-27

As of November 4, 2022, the federal government has moved ahead with its proposed and long-awaited update to Canada's private-sector privacy legislation, the *Digital Charter Implementation Act, 2022* ("**DCIA**").[1] The DCIA will bring about major changes to privacy law in Canada, impose new requirements on businesses, and provide for the imposition of significant financial penalties. The DCIA will enact two new laws, the *Consumer Privacy Protection Act* ("**CPPA**") and the *Artificial Intelligence and Data Act* ("**AIDA**"), create a new Personal Information and Data Protection Tribunal (the "**Tribunal**"), and amend the existing federal privacy law, the *Personal Information and Electronic Documents Act* ("**PIPEDA**"). While the DCIA is very similar to the 2020 version, there are changes that businesses should be aware of. Further, given that Bill-C27 is now one step ahead in the legislative process, at the second reading stage, it is worth reviewing this important proposed legislation.

The *Consumer Privacy Protection Act*: Significant Changes to PIPEDA

The DCIA's proposed changes to the current PIPEDA framework will provide individuals with increased protection of, and more control over their personal information, as well as greater transparency when organizations handle their personal information. In its Part 1, the CPPA provides for the obligations of organizations and will require businesses to implement and maintain a comprehensive privacy management program, provides for express consent and for exceptions to that requirement. It imposes requirements for the retention and disposal of personal information, and for providing individuals with access to and the right to amend personal information.

---

[1] As discussed in my December, 2020 report, at https://caobrienlaw.com/wp-content/uploads/2020/12/CAOB-Privacy-Bill-C-11-Dec-2020.pdf, the DCIA was introduced in 2020 as Bill C-11. However, that bill died when the September 2021 federal election was called. For the full text and an updated report on the current status of Bill C-27, see the Parliament of Canada's LEGISinfo site at: https://www.parl.ca/legisinfo/en/overview.

In Part 2, it provides for expanded powers of the Privacy Commissioner of Canada (the "**Commissioner**") with respect to dealing with complaints, conducting investigations and formal inquiries, and for the imposition of administrative monetary penalties ("**AMPs**"). Such AMPs can be up to the greater of $10 million or 3% of global gross revenues for contraventions of the CPPA, and for certain new offences, of the greater of $25 million or 5% of the organization's gross global revenues can be imposed by the Tribunal. In addition, the CPPA establishes a new private right of action for individuals who are affected by an act or omission of the organization that constitutes a contravention of the CPPA. Before the individual can initiate a lawsuit to recover damages for loss or injury suffered as a result of the contravention, the Commissioner and the Tribunal must have made findings that the organization has contravened the CPPA, and the finding was either not appealed to the Tribunal or the Tribunal had denied the appeal.

Changes will align the framework with that of the European Union's General Data Protection Regulation ("**GDPR**") and with Quebec's recently enacted Bill 64 amendments to its provincial private-sector privacy law.

As summarized in the federal government's updated guidance,[2] the DCIA will provide for:

- Increasing control and transparency for Canadians when their personal information is handled by organizations;
- Giving Canadians the freedom to move their information from one organization to another in a secure manner;
- Ensuring that Canadians can request that their information be disposed of when it is no longer needed;
- Establishing stronger protections for minors, including by limiting organizations' right to collect or use information on minors and holding organizations to a higher standard when handling minors' information;

---

[2] Innovation, Science and Economic Development Canada, "Bill C-27 summary: Digital Charter Implementation Act, 2022", August 18, 2022, posted at: https://ised-isde.canada.ca/site/innovation-better-canada/en/canadas-digital-charter/bill-summary-digital-charter-implementation-act-2020 [sic, the year 2020 is used in the 2022 summary].

- Providing the Privacy Commissioner of Canada with broad order-making powers, including the ability to order a company to stop collecting data or using personal information; and
- Establishing significant fines for non-compliant organizations — with fines of up to 5% of global revenue or $25 million, whichever is greater, for the most serious offences.

The privacy management program that each business must implement and maintain must be more than a mere privacy policy. Organizations will need to adopt practices and procedures for protecting personal information, including how it will deal with requests for information and complaints, how it will train and provide information to staff, and it will be required to develop materials to explain its policies and procedures to fulfil its obligations under the CPPA. The program must be drafted in plain language that the individual would reasonably be expected to understand. The program must reflect the volume and sensitivity of the personal information under the control of the organization. Additional protections are afforded to the personal information of minors as sensitive personal information. The Commissioner will have the authority to review privacy management programs upon request.

In general, organizations must obtain an individual's consent for the collection, use or disclosure of the individual's personal information, and that consent must be obtained at or before the time of the collection, or if the information is to be used or disclosed for a new purpose, before the use or disclosure for that other purpose. For consent to be valid, the organization must have provided a plain language description of: the purposes for the collection, use or disclosure of the personal information; the way in which the personal information is to be collected, used or disclosed; any reasonably foreseeable consequences of the collection, use or disclosure of the personal information; the specific type of personal information that is to be collected, used or disclosed; and the names of any third parties or types of third parties to which the organization may disclose the personal information.

The CPPA generally requires consent to be express. However, organizations will be permitted to collect and use (but not disclose) personal information without consent if it is for a business activity for which the organization has a "legitimate interest" that outweighs the potential adverse effect on the individual. This exception will apply only

where the organization has conducted and documented a privacy impact assessment confirming that the necessary conditions will exist.

The CPPA distinguishes between anonymizing and de-identifying personal information. In general, the CPPA will not apply to the former, defined as personal information that has been "irreversibly and permanently modified in accordance with generally accepted best practices to ensure that no individual can be identified from the information, whether directly or indirectly by any means". However, the protections will continue to apply to de-identified personal information, that "has been modified so that an individual cannot be directly identified from it, although a risk of the individual being identified remains".

Other issues addressed by Part 1 of the CPPA include: the organization's retention and disposal of personal information; accuracy of personal information; security safeguards including requirements that apply in the event of data breaches; openness and transparency; access to and amendment of personal information; the mobility of personal information; challenges to an organization's compliance; and the de-identification of personal information.

Artificial Intelligence and Data Act

At Part 3, Bill C-27 sets out the text of the AIDA. This new statute is intended to "regulate the international and interprovincial trade and commerce in artificial intelligence systems by establishing common requirements, applicable across Canada, for the design, development and use of those systems" and to "prohibit certain conduct in relation to artificial intelligence systems that may result in serious harm to individuals or harm their interests" (s. 4).

The AIDA defines an artificial intelligence system as a "technological system that, autonomously or partly autonomously, processes data related to human activities through the use of genetic algorithm, a neural network, machine learning or another technique in order to generate content or make decisions, recommendations or predictions." Such AI systems will be subject to detailed requirements with respect to the use of anonymized data, and require businesses using AI systems to conduct assessments as to whether AI systems are high impact systems (a term that will be defined in regulations). The AIDA also imposes detailed obligations for risk mitigation, monitoring, record keeping, and for plain-language disclosure to the public describing

how the system will be used. The AIDA regulates the types of content to be generated and the decisions, recommendations, or predictions to be made using AI systems. Businesses will be required to take mitigation measures to reduce the risk of harm or biased output.

Ministerial orders can be issued for the provision of documents and information and for audits. Enforcement mechanisms include AMPs and criminal offences. Details with respect to AMPs, including the range of amounts, factors to be considered, and possible defences will be established by regulations. For the AIDA's criminal offences, fines of the greater of $10 million and 3% of global gross revenues (on indictment) and of $5 million and 2% of global gross revenues (on summary conviction) are possible.

Next Steps

At the end of the second reading stage, Bill-27 will proceed to committee review, and further debate and consideration by both the House of Commons and the Senate. Given the importance of the proposed changes, public consultations are likely to be held, giving the OPC, businesses, industry associations and consumer groups the opportunity to comment on the proposed legislation. These consultations may result in changes to the legislation, or in delays in its implementation. Based on past practice, it is likely that the coming-into-force date will be from 12 to 18 months after the legislation has been adopted by both houses of Parliament and received royal asset. Businesses should anticipate having time to prepare to comply with the new laws, but should monitor the progress of the DCIA and begin to consider changes that will need to be made in respect of their collection, use and disclosure of personal information.

Please address any questions about these proposed changes, or about other privacy or advertising and marketing issues, to Carol Anne O'Brien at caob@caobrienlaw.com, or (416) 640-7270.

Carol Anne O'Brien's law practice is focused on regulatory matters including communications law (broadcasting and telecommunications), competition law, advertising and marketing, and privacy.