CAOB
CAROL ANNE O'BRIEN
BARRISTER & SOLICITOR

OFFICE 416·640·7270 MOBILE 416·399·6270 EMAIL caob@caobrienlaw.com FAX 416·368·5655 WEB caobrienlaw.com
151 Yonge Street, Suite 1500 Toronto, ON M5C 2W7

December, 2020

Major Changes to Privacy Law Proposed, Bill C-11

The federal government has introduced Bill C-11, the *Digital Charter Implementation Act, 2020* ("**DCIA**")[1] which, if enacted, would significantly amend Canada's private-sector privacy law, the *Personal Information and Protection of Electronic Documents Act* ("**PIPEDA**"). The DCIA would impose new obligations on businesses that collect, use and disclose the personal information of Canadians, along with fines of up to $10 million or 3% of global revenues. It will be important to monitor the progress of this legislation as it proceeds through committee review and subsequent stages before adoption.

Significant Changes to PIPEDA

Changes to PIPEDA legislative framework are intended to provide individuals with increased protection of, and more control over their personal information, as well as greater transparency when organizations handle their personal information. As proposed, the DCIA will provide for:[2]

- Updated consent rules, to ensure that individuals have the plain-language information needed to make choices about their personal information;
- Data mobility: individuals will have the right to direct the transfer of their personal information from one organization to another;
- The right of individuals to require the disposal of personal information and to withdraw consent;
- New transparency requirements for automated decision-making systems;

---

[1] Bill C-11 was introduced and received First Reading on November 17, 2020 and was tabled for Second Reading on November 24, 2020. Its full text and a report on its current status is available on the Parliament of Canada's LEGISinfo site at: https://www.parl.ca/LegisInfo/BillDetails.aspx?Language=E&billId=10950130

[2] Innovation, Science and Economic Development Canada, "Fact Sheet: Digital Charter Implementation Act, 2020", November 17, 2020, posted at: https://www.ic.gc.ca/eic/site/062.nsf/eng/00119.html.

- Clarification of requirements for organizations in connection with “de-identified information”;
- Expanded powers for the Privacy Commissioner of Canada and the Office of the Privacy Commissioner (“**OPC**”), including the ability to require organizations to comply with the CPPA and the ability to order a company to stop collecting data or using personal information;
- Providing for organizations to apply to the OPC for approval of codes of practice and certification systems that set out rules for how the CPPA could apply to certain activities, sectors or business models, demonstrating compliance with the new requirements;
- Simplifying consent by removing the burden to obtain consent when it would not provide any meaningful privacy protection; and
- Strengthened enforcement and oversight by a new Personal Information and Data Protection Tribunal (the “**Tribunal**”). The Tribunal will have the authority to impose administrative monetary penalties (“**AMPs**”) of up to 3% of global revenues or $10 million. The DCIA will also contain an expanded range of offence provisions for serious contraventions of the law, subject to fines of up to 5% of global revenues or $25 million.

Proposed New *Consumer Privacy Protection Act*

In Part 1, the DCIA would enact a new *Consumer Privacy Protection Act* (“**CPPA**”), which would increase the protection provided to Canadians’ personal information by requiring businesses to implement a “privacy management program” and provide greater transparency with respect to their activities relating to personal information. A privacy management program will involve more than 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.

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. In general, consent must be express. Implied consent is available only where the organization can establish that it is appropriate, taking into account the reasonable expectations of the individual and the sensitivity of the personal information that is to be collected, used or disclosed. An organization must not require consent, beyond that which is necessary to provide a particular product or service, as a condition of supplying the product or service.

There are exemptions to the requirement for consent, including for a “business activity” (as specified in the CPPA) where a reasonable person would expect such collection or use for that activity and the personal information is not collected and used for the purpose of influencing the individual’s behaviour or decisions. Organizations may transfer an individual’s personal information to a service provider without the individual’s knowledge or consent. Organizations may use an individual’s personal information without their knowledge or consent to de-identify the information, as well as for research and development purposes if the information is de-identified before it is used. There are a number of additional exemptions, including those that relate to business transactions, to personal information collected, used and disclosed in connection with an employment relationship where the organization operates a federal work, and to legal proceedings.

Additional issues addressed by 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 and use of that de-identified information.

Proposed Tribunal, Significant New Fines and Enforcement Powers

In Part 2, the DCIA would create a new Personal Information and Data Protection Tribunal (the "**Tribunal**"), which would have the power to hear appeals of certain decisions made by the OPC and to impose significant new penalties for the contravention of certain of its provisions.

Under the proposed regime, the OPC will continue to combine its current roles as an investigator, prosecutor and decision-maker. Its investigations will take place in two phases: investigations and inquiries. Where an investigation is followed by an inquiry, new remedies are possible, including compliance orders, AMPs, and private actions. With respect to AMPs and other remedies, the OPC will make recommendations to the Tribunal, which will make the final determinations and issue orders. The Tribunal will have the authority to impose penalties of up to 3% of an organization's global gross revenues or $10 million, whichever is larger.

Bill C-11 also includes criminal offence provisions, which would be punishable by fines of up to $25 million or 5% of global revenues, whichever is greater. The Tribunal will also hear appeals of decisions as made by the Commissioner. Bill C-11 also provides that, where the OPC or Tribunal has made a finding that an organization has contravened the CPPA, individuals who have suffered loss or injury will have the right to file private actions for damages. This private right of action will include the right to proceed through class actions.

Next Steps

Public consultations are likely to be held during committee review of Bill C-11, following second reading. The OPC, businesses, industry associations and consumer groups will have the opportunity to provide comment on specific details of the proposed legislation. These consultations may result in changes being made to the legislation, or in delays in implementing it.

Given that the Liberal government is a minority government, and in light of the priority being given to measures to address the Covid-19 pandemic, it is possible that Bill C-11 may not be enacted before a federal election. Further, the government has indicated

that the coming-into-force date will be from 12 to 18 months after the legislation has been adopted by Parliament and approved through royal asset.

Accordingly, while it is important for businesses to be aware of the potential impact of the DCIA and to consider changes that will need to be made in respect of its collection, use and disclosure of personal information, it is likely too soon for businesses to adopt specific new procedures to comply with the detailed requirements of the proposed CPPA.

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.