Bill C-11: A Closer Look (Part 2 of 2)

Proposed Acts and Proposed Changes to Requirements on Organizations and the Enforcement Regime

Fraser Mann and Anna Troshchynsky January 27, 2021

This is Part 2 of a two-part commentary describing some of the major substantive changes to Canada's privacy law set out in Bill C-11 (the "Bill), the Digital Charter Implementation Act, 2020. The Bill provides for the enactment of the *Consumer Privacy Protection Act* (the "CPPA") together with the enactment of the *Personal Information and Data Protection Tribunal Act* (the "PIDPTA"). Part 2 reviews the proposed requirements on organizations, the enforcement regime and penalties for non-compliance set out in the Bill.

Part 1 of the commentary is available here.

Note that the information presented here is based upon the first reading of the Bill tabled in the House of Commons on November 17, 2020 and is subject to change, as the Bill may be amended as it goes through the legislative process before becoming law.

Requirements on Organizations

While some of the obligations on Canadian private sector organizations under the *Personal Information Protection and Electronic Documents Act* ("PIPEDA") remain unchanged in the CPPA, there are new proposed requirements that, if passed, will impact organizations' privacy practices. An "organization" under the CPPA includes an association, a partnership, a person or a trade union.

The key requirements are highlighted below.

Implementing a Privacy Management Program

The CPPA mandates an organization to implement a privacy management program comprised of policies, practices and procedures directed at fulfilling its obligations under the CPPA, including (section 9 of the CPPA):

(i) protecting personal information;

(ii) responding to requests for information and complaints;

(iii) training and communicating to staff information about the organization's policies and practices; and

(iv) developing external materials to explain organization's policies and procedures.

The organization must also provide its privacy management program to the Privacy Commissioner of Canada (the "Commissioner") upon request (section 10 of the CPPA).

Pursuant to the accountability principle, an organization subject to PIPEDA is required to implement policies and practices concerning these four aforementioned elements (Principle 4.1.4

of PIPEDA). However, the CPPA requires an organization to specifically consider, when developing its privacy management program, the volume and sensitivity of the personal information in its control. This new requirement highlights the contextual approach an organization will have to take to comply with its obligations under the CPPA.

Identifying and Recording the Purposes of Collection, Use or Disclosure

An organization subject to PIPEDA may only collect, use or disclose personal information for the purposes that a reasonable person would consider appropriate in the circumstances (section 5(3) of PIPEDA). The CPPA, while having the same purpose requirement, goes further to codify five factors that the organization must consider when deciding whether such purposes are appropriate (section 12(2) of the CPPA):

(i) the sensitivity of the personal information;

(ii) the legitimate business needs of the organization;

(iii) the effectiveness of the collection, use or disclosure in achieving those business needs;

(iv) whether there are less intrusive means of achieving those purposes at a comparable cost and with comparable benefits; and

(v) whether the individual's loss of privacy is proportionate to the benefits in light of organization's security measures to mitigate the impacts of the loss of privacy on the individual.

Once the organization completes its assessment, it must record *each* of the identified purposes for which personal information will be collected, used or disclosed, and this must be done either at or before collecting such information (section 12(3) of the CPPA). Where personal information that was already collected will be used or disclosed for a new purpose, the organization must record the new purpose before using or disclosing the information (section 12(4) of the CPPA).

In order to comply with this new record keeping obligation, organizations will have to re-evaluate their handling of personal information and establish mechanisms to document the appropriate purposes for their collection, use and disclosure of the information.

Porting and Disposing of Personal Information

The CPPA affords individuals new rights to request an organization to (i) port the personal information it has collected about them to another designated organization (section 72 of the CPPA); and (ii) dispose their personal information that the organization has collected (section 55 of the CPPA). See Part 1 of the commentary for more information about these rights.

In order to comply with these individual rights, an organization will have to establish new internal processes and provide personnel training to handle individuals' requests to port and delete data. An organization that holds large amounts of personal information would also need to conduct a technical assessment of its information technology systems to determine whether individuals' requests can be fulfilled "as soon as feasible" as contemplated in the CPPA.

Other Requirements around Transparency

The CPPA establishes new requirements on organizations to promote greater transparency around automated decision making, third party data transfers and cross-border data flows.

An organization that uses automated decision systems to make a prediction, recommendatory or decision about an individual must, on request by the affected individual, provide an explanation about the process (section 63(3) of the CPPA). An organization would also have to provide, in plain language, a general account of its use of any automated decision system that could have significant impacts on individuals (section 62(2)(b) of the CPPA). See Part 1 of the commentary for additional detail about algorithmic transparency.

When an organization seeks an individual's consent for the collection of their personal information, it has to provide the names of any third parties or types of third parties to which personal information may be disclosed (section 15(3)(e) of the CPPA). An organization must also make readily available information on whether it carries out any international or interprovincial transfer or disclosure of personal information that may have reasonably foreseeable privacy implications (section 62(2)(d) of the CPPA). The CPPA does not include much more detail about this cross-border data transfer requirement.

Broad Order-Making Powers

The CPPA introduces a new order-making power where the Commissioner may order an organization to comply with the law. For example, the Commissioner may order an organization to cease collecting and using personal information that violates the CPPA. Furthermore, the Commissioner may order an organization to make public any measures taken or proposed to be taken to correct its policies, practices or procedures in order to comply with the law (section 92(2) of the CPPA).

Penalty Recommendations

The Commissioner may also make recommendations based on enumerated factors as to the penalty for non-compliance (section 93 of the CPPA). Among the factors to be considered in determining the amount of any penalty to be recommended are:

(i) the nature and scope of the contravention;

(ii) whether the organization has voluntarily paid compensation to a person affected by the contravention; and

(iii) the organization's history of compliance with the CPPA.

Any recommendation by the Commissioner to impose a penalty for non-compliance must be filed with the Personal Information and Data Protection Tribunal (the "Tribunal"), the role and duties of which are described in greater detail below.

Order-Making Powers in General

Currently, under PIPEDA, the Commissioner may only issue non-binding recommendations for an organization to implement and has no power to recommend monetary penalties.

The expansion of the Commissioner's powers is a welcomed change to effectively promote an organization's compliance with its privacy obligations. The grant of a direct order-making power

to the Commissioner is consistent with the powers granted to Privacy Commissioners in other jurisdictions, and has long been advocated by privacy professionals.

Establishment of a New Administrative Tribunal

Under the PIDPTA, the Tribunal is empowered to:

(i) impose penalties, by order, for non-compliance under the CPPA (section 94 of the CPPA); and

(ii) adjudicate appeals of the Commissioner's decisions and orders filed by affected complainants or organizations (section 100 of the CPPA).

The hearings of the Tribunal will be public and its decisions, along with the reasons for them, will also be made public (sections 15(4) and 18 of the PIDPTA). Operationally, the Tribunal will consist of three to six appointed members, where at least one of the members must have experience in the field of information and privacy law (section 6 of the PIDPTA).

The establishment of the Tribunal provides a mechanism for organizations and affected individuals to seek a review of the Commissioner's decisions in an expedited manner before turning to the Federal Court.

Substantial Penalties for Non-Compliance

Organizations may be subject to substantial penalties for contravention of the CPPA where the Tribunal, after receiving a penalty recommendation from the Commissioner, determines it is appropriate. The maximum penalty is the higher of $10 million CAD and 3% of the organization's gross global revenue in the financial year previous to that in which the penalty is imposed (section 94(4) of the CPPA). The Tribunal may substitute the Commissioner's findings with its own findings to vary the penalty.

Serious Contravention Offences

Section 125 of the CPPA introduces additional penalties on organizations that knowingly contravene specific obligations under of the CPPA.

Specifically:

(i) reporting breaches of an organization's security safeguards and notifying affected individuals (section 58 of the CPPA);

(ii) maintaining records of breaches of security safeguards (section 60(1) of the CPPA);

(iii) retaining information subject to an access request (section 69 of the CPPA);

(iv) restricting use of de-identified information (section 75 of the CPPA);

(v) whistleblower protections (section 124(1) of the CPPA); or

(vi) compliance with the Commissioner's order (section 92(2) of the CPPA);

may be subject to a fine up to the higher or $25 million CAD and 5% of the organization's gross global revenue if the matter is treated as an indictable offence, or a fine of up to the higher of $20

million CAD and 4% of organization's gross global revenue, if the matter is treated as a summary offence.

These proposed penalties in the CPPA are a different order of magnitude than the fines under the present law. Currently, PIPEDA imposes fines of up to $100,000 on organizations for knowingly failing to report breaches of security safeguards or for failing to maintain records of breaches. The penalties in the CPPA are akin to those in the European Union, where organizations subject to the *General Data Protection Regulation* ("GDPR") may face administrative fines of up to 20 million EUR or 4% of their annual global turnover of the preceding fiscal year, whichever is higher, for serious violations.

Private Right of Action

The Bill introduces a new private right of action, whereby an individual may bring an action against an organization for damages for loss or injury suffered as a result of that organization's contravention of the CPPA (section 106 of the CPPA). This right of action arises after: (i) the Commissioner has rendered a non-compliance decision that has not been overturned by the Tribunal; or (ii) the Tribunal has made a finding of violation. The action must be brought in the Federal Court of the applicable Provincial Superior Court within two years of any such decision or finding.

Presently, under PIPEDA, only the complainant may be awarded damages on application to the Federal Court following the Commissioner's investigation of his or her complaint. The Bill proposes to allow any individual who has suffered damages due to an organization's violation of the CPPA to bring an action. This new right of action is similar to Article 82(1) of the GDPR whereby any person that suffered damage as a result of non-compliance of a data controller or processor with the law has the right to compensation.

Code of Practice and Certification Program

An organization is granted the right under the CPPA to apply to the Commissioner for approval of a code of practice that provides substantially the same or greater level of protection of personal information as that provided under the CCPA (section 76 of the CPPA).

An organization may also apply to the Commissioner for approval of a certification program that includes (section 77 of the CPPA):

(i) a code of practice;

(ii) guidelines for interpreting and implementing the code of practice;

(iii) a mechanism by which organizations may be certified in compliance with the code of practice;

(iv) a mechanism to independently verify an organization's compliance with the code of practice;

(v) disciplinary measures for non-compliance with the code of practice; and

(vi) other requirements provided in the regulations.

The provisions dealing with codes of practice and certification programs are intended to encourage sectoral self-regulation as a means of complying with the obligations under the CPPA.

Although the establishment of a certification program is voluntary, it is possible for an association or licensing body to make compliance with the code of practice a condition of membership or a condition for being licensed by the licensing body. For example, an association representing dental professionals could apply for approval of a code of practice that deals specifically with the data processing activities or systems used by dental professionals, and that may provide specific types of protection to customers of dental clinics. A licensing body could also require compliance with the code of practice a condition for organizations that wish to supply goods or services to members of the association or licensing body.

The CPPA also allows the Commissioner to request an entity operating an approved certification program to provide information relating to the program to the Commissioner (section 122(k) of the CPPA). This may mean that an unincorporated industry group that is not otherwise subject to the CPPA may be required, for example, to provide reports about its compliance with the CPPA.

The regulations to be adopted under the CPPA will set out the criteria for approval of a certification program that includes a code of practice, and the process for submitting an application for approval of the program (section 122 of the CPPA).

Compliance with the requirements set out in an approved code of practice or certification program does not relieve an organization of its obligations under the CPPA (section 80 of the CPPA). However, the Commissioner is prohibited from recommending a penalty under the new law where, at the time of the contravention, the Commissioner finds the organization was in compliance with an approved certification program (section 93(3) of the CPPA).

The establishment of industry-developed codes of practice and certification programs pursuant to the CPPA is comparable to the GDPR's codes of conduct and data protection certification mechanisms that are aimed to assist data controllers and data processors demonstrate compliance and sectoral best practices (Articles 40-43 of the GDPR).

Concluding Comments

The new proposed requirements on organizations in the CPPA are intended to increase protections for Canadians' personal information and enhance transparency around organizations' privacy practices.

The penalties for non-compliance and the new enforcement mechanisms set out in the CPPA and the PIDPTA would ensure that Canada meets the requirements of the GDPR relating to its adequacy of the privacy laws in order to permit the unimpeded transfer of personal information as between countries in the European Union and Canada. The private right of action created by the new law allows individuals to seek damages for any loss or injury suffered as a result of any non-compliance with the CPPA.

If enacted as part of Canadian law, the new regime will result in Canada meeting the highest international standards for the protection of personal information.