LIBRARY OF PARLIAMENT
BIBLIOTHÈQUE DU PARLEMENT

PRELIMINARY VERSION

UNEDITED

The preliminary version of this Legislative Summary is made available to parliamentarians, parliamentary staff and the public to ensure timely access to the information, research and analysis needed to study the bill in question. The official version of the Legislative Summary, which may differ from this unedited version, will replace this document on the Parliament of Canada website.

LEGISLATIVE SUMMARY

BILL C-11:
AN ACT TO ENACT THE CONSUMER PRIVACY PROTECTION ACT AND THE PERSONAL INFORMATION AND DATA PROTECTION TRIBUNAL ACT AND TO MAKE CONSEQUENTIAL AND RELATED AMENDMENTS TO OTHER ACTS

43-2-C11-E

10 December 2020

Sabrina Charland, Alexandra Savoie and Ryan van den Berg

Parliamentary Information and Research Service

AUTHORSHIP

10 December 2020	Sabrina Charland	Legal and Social Affairs Division
	Alexandra Savoie	Economics, Resources and International Affairs Division
	Ryan van den Berg	Economics, Resources and International Affairs Division

ABOUT THIS PUBLICATION

Library of Parliament Legislative Summaries summarize bills currently before Parliament and provide background about them in an objective and impartial manner. They are prepared by the Parliamentary Information and Research Service, which carries out research for and provides information and analysis to parliamentarians and Senate and House of Commons committees and parliamentary associations. Legislative Summaries are revised as needed to reflect amendments made to bills as they move through the legislative process.

For clarity of exposition, the legislative proposals set out in the bill described in this Legislative Summary are stated as if they had already been adopted or were in force. It is important to note, however, that bills may be amended during their consideration by the House of Commons and Senate, and have no force or effect unless and until they are passed by both houses of Parliament, receive Royal Assent, and come into force.

Any substantive changes in this Library of Parliament Legislative Summary that have been made since the preceding issue are indicated in **bold print**.

Legislative Summary of Bill C-11
(Preliminary version)

43-2-C11-E

Ce document est également publié en français.

CONTENTS

LEGISLATIVE SUMMARY OF BILL C-11: AN ACT TO ENACT THE CONSUMER PRIVACY PROTECTION ACT AND THE PERSONAL INFORMATION AND DATA PROTECTION TRIBUNAL ACT AND TO MAKE CONSEQUENTIAL AND RELATED AMENDMENTS TO OTHER ACTS

1 BACKGROUND

On 17 November 2020, the Minister of Innovation, Science and Industry introduced Bill C-11 in the House of Commons.[1] The bill creates two new pieces of legislation: the Consumer Privacy Protection Act (the CPPA) and the Personal Information and Data Protection Tribunal Act (the Tribunal Act). The bill repeals Part 1 of the *Personal Information Protection and Electronic Documents Act* (PIPEDA) and changes the short title of that Act to the Electronic Documents Act.

This is the first bill to fully reform the federal private sector privacy legislation since PIPEDA was adopted in 2000.[2]

In general, the CPPA:

- codifies the contents of the fair information principles set out in Schedule 1 of PIPEDA by reformulating them as legislative provisions;
- maintains valid consent as the legal basis for the collection, use or disclosure of personal information by an organization (section 15);
- includes several exceptions to consent, including two new exceptions related to the business activities of an organization and the disclosure of personal information for socially beneficial purposes (sections 18 and 39);
- includes the right to erasure (section 55);
- includes the concept of algorithmic transparency, in the form of a right to explanation concerning decisions made by an automated decision system (sections 62 and 63);
- includes the concept of data portability, in the form of an ability for two organizations to disclose personal information between them in accordance with a data mobility framework (section 72);
- includes obligations concerning the de-identification of personal information (sections 74 and 75);

- grants the Privacy Commissioner (the Commissioner) additional powers, including the ability to make decisions, issue orders and recommend that the new administrative tribunal created by the bill impose a maximum penalty of the higher of $10,000,000 and 3% of an organization's gross global revenue (sections 92 and 93); and
- provides for a fine not exceeding the higher of $25,000,000 and 5% of the organization's gross global revenue in the case of a conviction for contravention of certain specific provisions of the CPPA or in the case of obstruction of the Commissioner's work (section 125).

As for the Tribunal Act, it establishes the Personal Information and Data Protection Tribunal and defines the internal operation and principles that inform its proceedings (the Tribunal).

1.1 CANADA'S DIGITAL CHARTER

The short title of the bill is the Digital Charter Implementation Act, 2020. Canada's Digital Charter (Charter) was unveiled by Innovation, Science and Economic Development Canada (ISED) in 2019.[3] The Charter is the result of consultations with many stakeholders beginning in June 2018.[4] The ten principles set out in the Charter include:

- control and consent;
- transparency, portability and interoperability; and
- strong enforcement and real accountability by imposing clear and meaningful penalties for violations of the laws and adopting regulations that support the principles set out in the Charter.

After releasing the Charter, ISED issued a discussion paper on PIPEDA reform, outlining issues and possible legislative amendments.[5] The bill appears to stem from those consultations.

1.2 CALLS FOR REFORM OF THE *PERSONAL INFORMATION PROTECTION AND ELECTRONIC DOCUMENTS ACT*

The bill follows up on several calls for reform, including by the Commissioner and the House of Commons Standing Committee on Access to Information, Privacy and Ethics (the committee).

For example, in his 2018–2019 annual report *Privacy Law Reform: A Pathway to Respecting Rights and Restoring Trust in Government and the Digital Economy*, the Commissioner recommended the modernization of federal privacy laws, including PIPEDA. Among other things, he recommended a rights-based approach for protecting

Canadians, proactive inspection powers without grounds and a privacy by design requirement.[6]

In his 2019–2020 annual report *Privacy in a Pandemic*, the Commissioner reasserted the need to reform our federal privacy laws, including PIPEDA. He noted that "[t]he law is simply not up to protecting our rights in a digital environment."[7] More recently, he made proposals for regulating artificial intelligence, including suggestions for legislative amendments to PIPEDA.[8]

The committee has recommended numerous amendments to PIPEDA in recent years, including in its 2018 report on the review of PIPEDA.[9] Numerous recommendations for modernizing PIPEDA were also made in the two reports that the committee published in 2018 as part of its review of the breach of personal information involving Facebook and Cambridge Analytica.[10]

The bill appears to address some of the past recommendations from the Commissioner or the committee, particularly by granting additional powers to the Commissioner, introducing a tougher monetary penalty regime and incorporating the concepts of data portability and algorithmic transparency into the CPPA.

1.3 ADEQUACY WITH THE EUROPEAN UNION

Under the European Union's *General Data Protection Regulation* (GDPR), personal data may be transferred to a third country or an international organization when the European Commission (EC) finds that the third party or international organization ensures an adequate level of protection.[11]

In 2001, under Directive 95/46/EC in effect at that time, the EC recognized that PIPEDA adequately protected personal data with respect to the disclosure of personal information in the course of commercial activities. That adequacy was reaffirmed in 2006.[12]

The GDPR replaces that Directive. It came into effect on 25 May 2018. It provides for the continuity of existing European Union (EU) adequacy decisions until they are reassessed.[13] Canada therefore maintains its adequacy status at this time. However, the EU must soon reassess the adequacy of the federal private sector privacy legislation with the GDPR.

The adequacy status ensures that data processed in accordance with the GDPR can be transferred from the European Union to Canada, or vice versa, without requiring additional guarantees concerning data protection (e.g., a contractual agreement).[14]

Since 2016, the EC is required to monitor the evolution of Canada's legal framework to determine whether Canada continues to ensure an adequate level of protection. The Government of Canada submits update reports to the EC regarding developments

in data protection law in Canada.[15] The exact date of the reassessment of Canada's adequacy status is not known, but the GDPR provides that there must be a reassessment every four years, meaning no later than 2022.[16]

2 DESCRIPTION AND ANALYSIS

The bill contains 37 clauses and is divided into three parts:

- Part 1 contains the full text of the new CPPA, the consequential and related amendments, terminology, transitional provisions and coordinating amendments (clauses 2 to 34).
- Part 2 contains the text of the Tribunal Act (clauses 35 and 36).
- Part 3 contains the coming into force provision (clause 37).

Other than clause 34, which contains coordinating amendments, the bill's provisions will come into force on a day to be fixed by order of the Governor in Council.

The following description highlights selected aspects of the bill; it does not review all of its provisions or those of the two Acts created by the bill.

2.1 THE CONSUMER PRIVACY PROTECTION ACT AND OTHER PROVISIONS (CLAUSE 2)

Clause 2 presents the CPPA as an Act "to support and promote electronic commerce by protecting personal information that is collected, used or disclosed in the course of commercial activities." It is divided into two parts.

Part 1 of the CPPA deals with the obligations of organizations related to the protection of personal information (sections 7 to 75). Part 2 of the CPPA deals with the Commissioner's powers, duties and functions and contains general provisions (sections 76 to 126).

The CPPA reiterates several elements of PIPEDA but in a structure that is more similar to a standard legislative text. The text of PIPEDA refers to fair information principles in its Schedule 1 (the principles set out in Schedule 1 of PIPEDA). These principles are not written in legislative language.[17] In the CPPA, these principles are incorporated in the text of the Act, using conventional legislative language.[18]

The CPPA imposes numerous obligations on the organization to which it applies, including the development of a privacy management program and data minimization obligations.

The relevant provisions of the CPPA are described in greater detail in the next pages.

2.1.1 Authorized Representatives (Section 4)

The CPPA states that the rights and recourses provided under the Act may be exercised by a person authorized by law to administer the affairs or property of a minor or a deceased individual, or by any person authorized in writing to do so by the individual. There is no such provision in PIPEDA.

2.1.2 Purpose (Section 5)

The purpose of the CPPA remains essentially the same as that of PIPEDA: to establish rules to govern the protection of personal information in a manner that recognizes the right of privacy of individuals and the need of organizations to collect, use or disclose personal information for purposes that a reasonable person would consider appropriate in the circumstances (section 5).

In his statement concerning the tabling of the bill, however, the Commissioner stated:

> Bill C-11 opens the door to new commercial uses of personal information without consent but does not specify that such uses are conditional on privacy rights being respected. Rather, the Bill essentially repeats the purpose clause of the current legislation, which gives equal weight to privacy and the commercial interests of organizations.[19]

Although the purpose remains essentially the same, the context in which these rules governing the protection of personal information are established has been modified to indicate that they are established "in an era in which data is constantly flowing across borders and geographical boundaries and significant economic activity relies on the analysis, circulation and exchange of personal information" (section 5).

2.1.3 Application (Section 6)

The CPPA applies to every organization in respect of personal information that it collects, uses or discloses in the course of commercial activities or the personal information of its employees (section 6(1)). This application is the same as that of PIPEDA.

However, under the CPPA, the definition of "commercial activity" has changed. It means "any particular transaction, act or conduct or any regular course of conduct that is of a commercial character, taking into account an organization's objectives for

carrying out the transaction, act or conduct, the context in which it takes place, the persons involved and its outcome" (section 2).

The title of the CPPA identifies the "consumer" as the beneficiary of the protections it sets forth. However, the term "individual" is used in the provisions of the CPPA.

The CPPA specifies that it applies in respect of personal information that is collected, used or disclosed interprovincially or internationally by an organization or within a province, unless it is exempt from the application of the CPPA under section 119(2)(b) (section 6(2)). Section 119(2)(b) sets forth the process by which a province may have its provincial legislation recognized as "substantially similar" to PIPEDA.[20]

The CPPA does not include an explicit provision concerning its extraterritorial application to organizations that are not established in Canada.[21]

2.1.4 Accountability of Organizations (Sections 7 to 11)

Under the CPPA, all organizations are accountable for personal information under their control.[22] Information is under the control of an organization when it determines the purposes for its collection, use or disclosure. The CPPA states that an organization maintains the accountability even if a service provider carries out these activities on its behalf. The obligations set out in the CPPA do not apply to a service provider for information transferred to it by an organization (unless it collects, uses or discloses it for another purpose). The organization must also ensure that a service provider to which it transfers personal information provides the same protection that it is required to provide under the CPPA (sections 7 and 11).

Each organization must designate at least one individual to be responsible for matters related to its obligations under the CPPA and implement a privacy management program (program). That program includes the policies, practices and procedures put in place by the organization to fulfil its obligations under the CPPA. It must take into account the volume and sensitivity of the personal information under the control of the organization (sections 8 and 9).

The organization must also, on request, provide the Commissioner with access to the program (section 10).

2.1.5 Appropriate Purposes for the Collection, Use and Disclosure of Personal Information and Applicable Limitations (Sections 12 to 14)

Sections 12 to 14 of the CPPA apply a necessity and proportionality test for the collection, use and disclosure of personal information.[23]

The CPPA states that an organization can only collect, use or communicate personal information "for purposes that a reasonable person would consider appropriate in the circumstances" (section 12(1)). It includes a list of factors to consider in determining whether the purposes are appropriate:

- the sensitivity of the personal information;
- whether the purposes represent legitimate commercial needs;
- the effectiveness of the collection, use or disclosure in meeting these needs;
- the existence of less intrusive means of achieving those purposes at a comparable cost and with comparable benefits; and
- whether the individual's loss of privacy is proportionate to the benefits.

The appropriate purposes must be determined at or before the time of the collection and the purposes must be recorded (section 12(3)). The CPPA does not state how they are to be recorded.

The organization may only collect, use or disclose personal information that is necessary for the purposes determined for collection. If it wants to use or disclose information gathered for a new purpose, it must record that new purpose and obtain the individual's valid consent, unless an exception to consent applies (sections 12(4), 13 and 14).

2.1.6 Consent (Sections 15 to 17)

Consent remains the default legal basis for an organization to collect, use and disclose personal information under the CPPA (section 15). Without consent, an organization must justify the collection, use or disclosure of personal information based on an exception. There are many exceptions to consent under the CPPA, which are summarized under subtitle 2.1.7.

Under the CPPA, consent is valid if the organization provides the individual with certain information in plain language (section 15(3)). This information includes:

- 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.

By contrast, PIPEDA provides that consent is valid if it is reasonable to expect that an individual "would understand the nature, purpose and consequences of the collection, use or disclosure of the personal information to which they are consenting" (section 6.1 of PIPEDA).

Under the CPPA, an organization may establish that implied consent is appropriate in certain circumstances, taking into account the reasonable expectations of the individual and the sensitivity of the personal information that is to be collected, used or disclosed (section 15(4)). An organization must not obtain or attempt to obtain an individual's consent using deceptive or misleading practices (section 16). Moreover, an individual may, at any time, withdraw their consent, with reasonable notice, and unless prevented by the CPPA, federal or provincial law or a "reasonable" contract (section 17).

2.1.7 Exceptions to Consent (Sections 18 to 52)

There are six categories of exceptions that allow for the collection, use or disclosure of personal information without the individual's knowledge or consent:

- the organization's business activities (sections 18 to 28);
- public interest (sections 29 to 39);
- investigations (sections 40 to 42);
- disclosures to government institutions (sections 43 to 48);
- required by law (sections 49 and 50); and
- publicly available information (section 51).

The exceptions set out in sections 23 to 38 and 40 to 51 substantially replicate the content of sections 7 and 7.2 to 7.4 and sections 10.2(3) and 10.2(4) in PIPEDA. The new exceptions contained in the CPPA are examined below.

A new exception to consent related to "business activities" allows an organization to collect or use personal information without the individual's knowledge or consent if

the collection or use is made for a business activity. The collection or use must also meet two conditions: a reasonable person would expect such a collection or use, and the personal information is not collected or used for the purpose of influencing the individual's behaviour or decisions (section 18).

The business activities covered by this exception include, for example, the organization's activities needed to provide or deliver a product for an individual, but also "an activity in the course of which obtaining the individual's consent would be impracticable because the organization does not have a direct relationship with the individual" (section 18(2)).

Under the CPPA, an organization may also transfer an individual's personal information to a service provider without their knowledge or consent (section 19). It can also use an individual's personal information without their knowledge or consent to de-identify the information (section 20). The term "de-identify" is defined in section 2 of the CPPA as follows:

> means to modify personal information – or create information from personal information – by using technical processes to ensure that the information does not identify an individual or could not be used in reasonably foreseeable circumstances, alone or in combination with other information, to identify an individual. (*dépersonnaliser*)

An organization may use de-identified information for its internal research and development purposes without the individual's knowledge or consent (section 21). It may also use or disclose personal information without consent as part of a prospective business transaction but, under the CPPA, that information must be de-identified (section 22).

The CPPA also includes a new exemption to consent that allows an organization to disclose personal information without the individual's knowledge or consent for a "socially beneficial purpose." This means "a purpose related to health, the provision or improvement of public amenities or infrastructure, the protection of the environment or any other prescribed purpose" (section 39). Information can only be disclosed for socially beneficial purposes if the following conditions are met:

- the information is de-identified;
- the information is disclosed to a public organization (government institution, health care institution or post-secondary educational institution or public library), an organization mandated under a federal or provincial law or by a prescribed entity; and
- the disclosure is made for a socially beneficial purpose.

Section 52 states that an organization cannot rely on certain exceptions to consent if it collects an individual's electronic address using a specialized computer system or personal information using a computer system in contravention of an Act of Parliament. It essentially reiterates the terms of section 7.1 of PIPEDA.

2.1.8 Retention, Disposal, Accuracy of Personal Information (Sections 53 to 56)

Sections 53 to 56 of the CPPA deal with the limitations that apply to the period for retention of personal information and the accuracy of such information.[24] Under those sections:

- personal information is only retained for the time needed to fulfil the purposes for which the information was collected, used or disclosed, or to comply with the requirements of the Act or of the reasonable terms of a contract (section 53);
- an organization that uses personal information to make a decision must retain the information for a sufficient period of time to permit the individual to make a request for information or access (section 54); and
- an organization must take reasonable steps to ensure that personal information under its control is up to date, accurate and complete, and the extent to which the information must be up to date, accurate and complete takes into account the individual's interests and other factors, such as whether the information is used to make a decision about the individual, whether the information is used on an ongoing basis, and whether the information is disclosed to third parties (section 56).

The CPPA introduces a new explicit right to dispose of personal information that an organization has collected from an individual (right to erasure). At an individual's request, the organization proceeds with disposal unless it would result in the disposal of personal information about another individual and the information is not severable, or there are legal requirements or reasonable terms of a contract that prevent it from doing so. If the organization refuses to dispose of an individual's personal information, it must inform the individual in writing of its refusal and its reasons and advise the individual of their right to file a complaint with the organization or the Commissioner.
The organization must also inform any service provider to which the information has been transferred of the request for disposal and obtain confirmation from the service provider that it has disposed of the information (section 55).

2.1.9 Security Safeguards (Sections 57 to 61)

Under the CPPA, an organization must protect the personal information that it holds.[25] Protection must be through physical, organizational or technological security safeguards and the level of protection must be proportionate to the sensitivity of the information.

The safeguards must also take into consideration the quantity, distribution, format and method of storage of the information (section 57).

The CPPA also imports the content of sections 10.1 to 10.3 of PIPEDA, which set forth a system for reporting breaches of security safeguards (sections 58 to 60).

That system requires an organization to report to the Commissioner any breach of security safeguards involving personal information under its control if it is reasonable in the circumstances to believe that "the breach creates a real risk of significant harm to an individual." It must also inform the individual as soon as possible (section 58). Significant harm includes, for example, bodily harm, humiliation and damage to reputation or relationships (section 58(7)).

An organization that notifies an individual of a breach of security safeguards must also notify any other organization or government institution that may be able to reduce or mitigate the risk of harm that could result from the breach (section 59). It must keep a record of breaches of security safeguards involving personal information and provide the Commissioner with access to the record on request (section 60). Any service provider that determines that a breach of security safeguards involving personal information has occurred must, as soon as feasible, notify the organization that controls the personal information (section 61).

2.1.10 Openness and Transparency (Section 62)

The CPPA requires that an organization make readily available information on its policies and practices aimed at complying with the Act.[26] The information that an organization must share includes:

- whether or not it carries out any interprovincial or international transfer or disclosure of personal information that may have reasonably foreseeable privacy implications; and
- a general account of the organization's use of "automated decision systems" to make predictions, recommendations or decisions about individuals that could have a significant impact on them.

The first piece of information requires an organization to share information about its cross-border flow of data, but only if it determines that it may have privacy implications for the individuals involved.

With respect to information that an organization must provide regarding its use of "automated decision systems," the term "automated decision system" is defined as follows in section 2 of the CPPA:

> Technology that assists or replaces the judgment of human decision-makers using techniques such as rules-based systems, regression analysis, predictive analysis, machine learning, deep learning and neural nets.

Section 62 therefore introduces the concept of algorithmic transparency into the CPPA, in the form of a right to explanation. That right to explanation is also found in section 63 of the CPPA.

2.1.11 Access to and Amendment of Personal Information (Sections 63 to 71)

On request by an individual, an organization must inform them of whether it has personal information about them, how it uses the information and whether it has disclosed it. If the organization has used an automated decision system to make a prediction, recommendation or decision about the individual, that individual may request an explanation from the organization. The organization must then indicate how the personal information used to make the prediction, recommendation or decision was obtained. The access request must be made in writing (sections 63 and 64).[27]

The CPPA introduces an obligation to provide all information requested by an individual in plain language (section 66). This should ensure that an organization does not provide lengthy documents using complex legal terms.

The organization must respond to the information request no later than 30 days after it is received, unless the organization informs the individual within 30 days of receipt of the request that the deadline will be extended (for a maximum of 30 additional days) or that a longer period is needed to convert the personal information to an alternative format. Any refusal to comply with the information request must be justified. In this case, the organization shall inform the individual and advise them of any recourse they may have (section 67). The organization may charge a minimal cost for processing a request (section 68). Personal information that is the subject of a request for information or access must be retained long enough to allow the individual to exhaust any recourse under the CPPA (section 69).

The organization must not give an individual access to personal information that reveals personal information about another individual, unless it is severable, if the other individual consents to the disclosure or if the requester needs the information because an individual's life, health or security is threatened (sections 70(1) and 70(2)).

If the individual asks an organization to inform them of any disclosure to a government institution under the exceptions to consent set out in sections 44 to 48 or 50 of the

CPPA or of the existence of any information that it has relating to such a disclosure, it must notify the government institution in question. The institution must inform the organization within 30 days of receipt of the request of whether it objects to the organization providing the desired information to the individual. The institution may only object in certain circumstances, such as cases in which it is of the opinion that compliance with the request for information or access could be injurious to national security or the enforcement of the law (sections 70(3) to 70(5)).

If there is an objection, the organization refuses to comply with the request for information or access, notifies the Commissioner in writing of the refusal and does not give the individual access to any information relating to a disclosure to a government institution. In that context, the organization does not provide the individual with the name of the government institution it notified and does not inform him of the institution's objection to the organization complying with the individual's request (section 70(6)).

The organization may also refuse to disclose personal information to an individual who requests information in certain specific cases (section 70(7)), namely if:

- the information is protected by solicitor–client privilege or the professional secrecy of advocates and notaries or by litigation privilege;
- disclosure would reveal confidential commercial information;
- disclosure could threaten the life or security of an individual;
- the information was collected without the individual's knowledge or consent in the course of an investigation into a breach of an agreement or a contravention of federal or provincial law and collecting it otherwise would have compromised the availability or the accuracy of the information;
- the information was only generated in the course of a formal dispute resolution process; or
- the information was created for the purpose of making a disclosure under the *Public Servants Disclosure Protection Act* or in the course of an investigation into such a disclosure.

With respect to amendment of personal information, if an individual has been given access to their personal information and demonstrates to an organization that it is outdated, inaccurate or incomplete, the organization must make the necessary amendments and, if appropriate, transmit the amended information to any third party that has access to the information. If there is disagreement between the organization and the individual concerning the amendments to be made, the organization must record the disagreement and the third parties must be informed (section 71).

2.1.12 Mobility of Personal Information (Section 72)

The CPPA introduces a right to mobility of personal information. It allows an individual to request that the personal information collected from them by an organization be transmitted to an organization chosen by the individual. However, that transfer is only allowed if both organizations involved are subject to a data mobility framework provided for in future regulations.

2.1.13 De-identification of Personal Information (Sections 74 and 75)

The CPPA provides that, when an organization de-identifies personal information, it must use technical and administrative measures that are proportionate to the purpose for which the information is de-identified and the sensitivity of the personal information. It does not define what is meant by "technical and administrative measures" (section 74). It also prohibits the use of de-identified information, alone or in combination with other information, to identify an individual. In other words, it prohibits the re-identifying personal information (section 75).

2.1.14 Codes of Practice and Certification Programs (Sections 76 to 81)

Under section 24 of PIPEDA, the Commissioner encourages organizations to develop detailed policies – particularly codes of practice – to comply with the requirements of the Act.

The CPPA includes a more comprehensive regime that allows an organization to ask the Commissioner to approve a code of practice or a certification program under criteria to be established by regulation. The certification program must include several elements, including a code of practice, guidelines for interpreting and implementing the code and a mechanism for the independent verification of an organization's compliance with the code. The Commissioner's decision to approve a code of practice or a certification program must be made public (sections 76 to 79). Compliance with a code of practice or a certification program does not relieve an organization of its obligations under the CPPA (section 80). Under that regime, the Commissioner has certain powers, for example, the authority to request information from any entity that manages a certification program or to revoke a certification program in accordance with the regulations (section 81).

2.1.15 Investigation of Complaints, Inquiries, Penalties and Appeals (Sections 82 to 95 and 100 to 105)

Sections 82 to 87 of the CPPA set out the complaint process under the Act and the circumstances in which the Commissioner can refuse to investigate a complaint or discontinue an investigation. They substantially replicate the content of sections 11, 12 and 12.2 of PIPEDA.[28] The CPPA, however, contains a new ground for the Commissioner to refuse to investigate a complaint as he or she deems it to be inadmissible, namely if "the complaint raises an issue in respect of which a certification that was approved by the Commissioner … and the organization is certified under that program" (section 83(1)(d)). The Commissioner may also discontinue the investigation of a complaint if the circumstances set out in section 83(1)(d) exists (section 85).

The Commissioner may attempt to resolve a complaint by means of mediation or conciliation and may enter into a compliance agreement with an organization, aimed at ensuring compliance with the CPPA (sections 84 and 86). If the Commissioner discontinues the investigation of a complaint, or if the Commissioner determines at the conclusion of the investigation that he or she will not be conducting an inquiry, the Commissioner must notify the complainant and the organization and give reasons (section 87).

The inquiry process under the CPPA replaces sections 14 to 17 of PIPEDA, which provided for the possibility of recourse before the Federal Court following the investigation of a complaint by the Commissioner and his or her report summarizing his or her findings and non-binding recommendations.

Under the CPPA, once the investigation of a complaint is completed, the Commissioner can give notice to the complainant and the organization that it will conduct an inquiry into the complaint. The Commissioner can also conduct an inquiry into whether there are reasonable grounds to believe that a compliance agreement has not been respected (sections 88 and 89). As part of an inquiry under the CPPA, the Commissioner is not bound by the legal or technical rules of evidence during the inquiry. He or she must instead attempt to act informally and expeditiously and is free to establish the procedure to be followed in conducting an inquiry. The Commissioner must make that procedure public (sections 90 and 91).

On completion of the inquiry, the Commissioner renders a decision that sets out his or her findings on whether the organization has contravened the Act or has not complied with a compliance agreement, any order made, or any recommendations to the Tribunal to impose a penalty. The decision must include reasons for his or her findings, orders or decisions (section 92). Under section 92(2) of the CPPA, the Commissioner can order an organization to:

- take measures to comply with the CPPA;
- stop doing anything that is in contravention of it;
- comply with the terms of a compliance agreement; or
- make public any measures it takes to correct its policies, practices or procedures for safeguarding personal information.

The order made by the Commissioner (or by the Tribunal in an appeal) may be made an order of the Federal Court for the purpose of its enforcement (sections 103 to 105).

The CPPA does not give the Commissioner the power to impose a penalty. Only the Tribunal can impose a penalty on the recommendation of the Commissioner or, in an appeal, on its own initiative if the Commissioner has not recommended it.

The Commissioner recommends a penalty if he or she finds that an organization has contravened one or more specific provisions of the CPPA.[29] The Commissioner must consider certain factors, including the nature and scope of the contravention, any voluntary compensation paid by the organization to the individual and the organization's history of compliance with the CPPA. The Commissioner cannot recommend a penalty if he or she is of the opinion that, at the time of the contravention of a provision of the CPPA, the organization was in compliance with the requirements of an approved certification program in relation to that provision (section 93).

Any decision, finding or order by the Commissioner shall be appealed before the Tribunal, which may dismiss or allow the appeal. In allowing the appeal, the Tribunal may substitute its own finding, order or decision for the one under appeal. The standard of review applicable to an appeal is set out in the CPPA (sections 100 to 102).

The Tribunal may, by order, impose a penalty on an organization if it has received a recommendation from the Commissioner or if, in an appeal under section 100(1) of the CPPA, it finds that it is appropriate to impose one even if the Commissioner has not recommended it. In deciding whether to impose a penalty on an organization, the Tribunal relies on the findings set out in the Commissioner's decision (or its own if it substitutes them for those of the Commissioner in an appeal) (sections 94(1) and 94(2)). A penalty cannot be imposed on an organization for a contravention of the CPPA if a prosecution for the act or omission that constitutes the contravention has been instituted against the organization or if it establishes that it exercised due diligence to prevent a contravention of the CPPA (section 94(3)).

The maximum penalty for all contraventions is the higher of "$10,000,000 and 3% of the organization's gross global revenue in its financial year before the one in which

the penalty is imposed" (section 94(4)). In determining the amount of the penalty, the Tribunal must consider the following factors:

- the factors to be considered by the Commissioner before making his or her recommendation to the Tribunal;
- the organization's ability to pay the penalty and the likely effect of paying it on the organization's ability to carry on its business; and
- any financial benefit that the organization obtained from the contravention of the CPPA.

The CPPA states that the purpose of a penalty is not to punish but to promote compliance with this Act (section 94(6)).

2.1.16 Audits
(Sections 96 and 97)

The Commissioner may, on reasonable notice, audit the personal information management practices of an organization if the Commissioner has reasonable grounds to believe that the organization has contravened Part 1 of the CPPA. After the audit, the Commissioner presents the findings and recommendations that the Commissioner considers appropriate in a report (sections 96 and 97).

2.1.17 Commissioner's Powers, Duties and Functions
(Sections 98, 99 and 108 to 118)

Most of the Commissioner's powers, duties and functions under the CPPA are the same as under PIPEDA.

For instance, in terms of investigations, inquiries and audits, the Commissioner can summon and enforce the appearance of witnesses before him or her or visit any premises occupied by an organization. However, under the CPPA, the Commissioner may also make an interim order or order an organization to retain relevant information for as long as is needed for an investigation, inquiry or audit (sections 98 and 99).

In addition, in carrying out his or her duties and functions, the Commissioner must also consider the purpose of the Act, the size and revenue of the organization, the volume and sensitivity of the personal information under their control and matters of general public interest (section 108).

The Commissioner maintains his or her mandate of promoting the purpose of the CPPA, but it can now also provide advice to an organization concerning its privacy management program (section 109). The Commissioner must also make public

information on the manner in which he or she exercises his or her duties and functions (section 111).

Under section 112, the Commissioner and persons acting on his or her behalf or under his or her direction must not disclose any information that they receive in carrying out almost all duties and functions set out in the CPPA. However, the Commissioner may, if he or she considers that it is in the public interest to do so, make public any information that comes to the Commissioner's knowledge in the exercise of any of his or her powers or the performance of any of his or her duties or functions under the Act (section 112(3)). The Commissioner can also disclose or authorize the disclosure of information in certain circumstances, for instance at a hearing or an appeal before the Tribunal or to the Attorney General of Canada, or if the Commissioner is of the opinion that there is evidence related to the commission of offences under federal or provincial law by an officer or employee of an organization (sections 112(4) to 112(8)).

The Commissioner and persons acting on behalf or under the direction of the Commissioner may only be called to testify on matters that come to their knowledge as a result of the exercise of their duties or functions under the CPPA in three circumstances: a prosecution for an offence under section 125 of the CPPA, a prosecution for an offence under the *Criminal Code* for perjury in respect of a statement made under the CPPA, or a proceeding or an appeal before the Tribunal (section 113).

No criminal or civil proceedings may be brought against the Commissioner or persons acting on behalf or under the direction of the Commissioner for anything done in good faith in exercising their duties. They also have immunity from defamation proceedings (section 114).

Under the CPPA, the Commissioner may enter into agreements or arrangements with the Canadian Radio-television and Telecommunications Commission (CRTC) or the Commissioner of Competition in order to undertake and publish research on issues of mutual interest (section 115). The Commissioner may consult with provincial counterparts to ensure that personal information is protected in as consistent a manner as possible and enter into agreements or arrangements with them, for example, to coordinate the activities of their respective offices by providing for mechanisms for the handling of any complaint in which they are mutually interested. Under the procedure set out in the agreement or arrangement, the Commissioner may also provide information that may be of use to his or her counterparts or assist them in carrying out their duties and functions to protect personal information (section 116).

The Commissioner may also disclose some information to a person or organization who, under the legislation of a foreign state, has powers, duties and functions similar

to those of the Commissioner or has responsibilities that relate to conduct that is substantially similar to conduct that would be in contravention of the CPPA. Information can only be disclosed if a written agreement has been entered into by the two parties (section 117).

The Commissioner tables in each House of Parliament an annual report concerning the application of the CPPA, the extent to which the provinces enacted substantially similar legislation and the application of such provincial legislation (section 118).

2.1.18 Private Right of Action (Section 106)

The CPPA introduces a private right of action. It gives an individual who is affected by an act or omission by an organization that has contravened the CPPA a cause of action for damages. Action can only be brought if the Commissioner or the Tribunal has found that the organization has contravened the CPPA or if the organization is fined for a contravention of the CPPA under section 125. A limitation period of two years applies to this right.

2.1.19 Fines (Section 125)

Section 125 provides that any organization that contravenes certain specific provisions of the CPPA (sections 58, 60(1), 69, 75 and 124(1)) or an order made by the Commissioner, or that obstructs the work of the Commissioner's office during an inquiry or audit is

> (a) guilty of an indictable offence and liable to a fine not exceeding the higher of $25,000,000 and 5% of the organization's gross global revenue in its financial year before the one in which the organization is sentenced; or
>
> (b) guilty of an offence punishable on summary conviction and liable to a fine not exceeding the higher of $20,000,000 and 4% of the organization's gross global revenue in its financial year before the one in which the organization is sentenced.

This represents a significant increase from the fines set out in section 28 of PIPEDA, in which the maximum fine for an offence under that Act was $100,000. These fines are not imposed by the Tribunal, but by the courts following prosecution for an offence at the discretion of the Attorney General of Canada.

2.1.20 General Provisions (Sections 119 to 124 and 126)

The Governor in Council may, by regulation, adopt any measures to apply the CPPA, for example, to govern the scope of the business activities set out in section 18 (section 119(1)(a)). The Governor in Council may also provide for certain things, by order, particularly which organizations are exempt from the application of the CPPA when provincial legislation recognized as being substantially similar to it applies (section 119(2)). The Governor in Council may also establish, by regulation, the criteria and processes for determining that a province has enacted substantially similar legislation and the processes for reconsidering that determination (section 119(3)).

The Governor in Council may also make regulations respecting the data mobility frameworks set out in section 72 and respecting the codes of practice and certification programs set out in sections 76 to 81 of the CPPA (sections 120 and 122). Regulations for applying the CPPA made under section 119(1) or section 120 may distinguish different classes of activities, government institutions and or parts of such institutions, information, organizations or entities (section 121).

Any person who has reasonable grounds to believe that another person has contravened or intends to contravene Part 1 of the CPPA may report that person to the Commissioner and request confidentiality (section 123). The CPPA prohibits an employer from dismissing, suspending, demoting, disciplining, harassing or otherwise disadvantaging an employee who, in good faith, informs the Commissioner of a contravention of the CPPA, refuses to do anything that is in contravention of Part 1 of the CPPA, or has done or stated an intention of doing anything that is required to prevent a contravention of Part 1 of the CPPA. This prohibition also applies if the employer believes that the employee will do one of the things noted above (section 124).

A parliamentary review of the CPPA is provided for every five years (section 126).

2.2 CONSEQUENTIAL AND RELATED AMENDMENTS, TERMINOLOGICAL AMENDMENTS, TRANSITIONAL PROVISIONS AND COORDINATING AMENDMENTS (CLAUSES 3 TO 34)

The bill makes consequential and related amendments to other Acts. It amends PIPEDA by repealing several parts of that Act and renaming it the Electronic Documents Act. The amendment reduces the Electronic Documents Act's scope to the use, by the federal government, of electronic means to record or communicate information (clauses 3 to 8). The content of the repealed parts of PIPEDA is reflected in parts 1 and 2 of the CPPA.

Consequential and related amendments are also made to other Acts to make reference to the CPPA and its relevant provisions or to the Tribunal, for example:

- Schedule II of the *Access to Information Act*, which identifies the provisions of other Acts that limit the disclosure of personal information and may thus justify a federal institution's refusal to disclose certain documents, is amended to strike out the reference to PIPEDA and its section 20(1.1) and to replace it with a reference to the CPPA and its section 112(2).
- Section 4.83(1) of the *Aeronautics Act*, which deals with information requests by foreign states, is amended to replace the reference to PIPEDA with a reference to Part 1 of the CPPA.
- Items 14 and 17 of the schedule to the *Canada Evidence Act* (which lists entities designated for the purposes of other Acts) are amended. The reference to PIPEDA in items 14 and 17 is replaced by a reference to the CPPA. Item 17 identifies the Personal Information and Data Protection Tribunal as the designated entity for the purposes of the CPPA, instead of the Federal Court.

The bill also amends the *Canadian Radio-television and Telecommunications Commission Act* and the *Competition Act* to give the CRTC and the Commissioner of Competition the power to enter into research agreements with the Privacy Commissioner and to develop procedures for disclosing information to the Privacy Commissioner (clauses 13 and 14).

A few other Acts are amended to replace any reference to PIPEDA with a reference to the CPPA and its relevant parts or provisions (sections 15 to 31). The bill also makes terminology amendments to 13 Acts to replace all references to PIPEDA with a reference to the Electronic Documents Act (clause 32).

The transitional provisions of the CPPA specify how a pending complaint will be dealt with once its section 82 comes into force. For example, a complaint initiated before it comes into force will be dealt with in accordance with PIPEDA. If the Commissioner has reasonable grounds to believe that the contravention in question is continuing after the initial date on which the complaint was filed, it is dealt with in accordance with the CPPA (clause 33).

2.3 PERSONAL INFORMATION AND DATA PROTECTION TRIBUNAL ACT (CLAUSES 35 AND 36)

Part 2 of the bill contains two clauses. The first enacts the Tribunal Act, thus creating the Tribunal (clause 35). The second provides for a related amendment to the *Administrative Tribunals Support Service of Canada Act* to add the Tribunal to the alphabetical list of administrative tribunals in the schedule to that Act (clause 36).

We provide a description of the provisions of the Tribunal Act.

2.3.1 Introductory Provisions and Definitions (Sections 2 and 3)

The Tribunal Act defines the minister responsible for applying the Act as a member of the Queen's Privy Council for Canada designated by order of the Governor in Council or, if there is no designation, the Minister of Industry (section 3).

2.3.2 Establishment and Jurisdiction of the Tribunal (Sections 4 and 5)

Section 4 of the Tribunal Act establishes the Tribunal. The Tribunal's jurisdiction is limited. It can only rule on all appeals made under section 100 or 101 of the CPPA or in respect of the imposition of penalties under section 94 of that Act (section 5).

Under section 100 of the CPPA, the Tribunal hears any appeals from an inquiry by the Commissioner with respect to a compliance order between the Commissioner and an organization or with respect to the Commissioner's decision not to recommend that a penalty be imposed on an organization that allegedly contravened the CPPA. On leave to appeal, it can also hear any appeals arising from an interim order that the Commissioner considers appropriate as part of a complaint, inquiry or audit (section 101 of the CPPA). Finally, the Tribunal has jurisdiction to impose a penalty on an organization when the conditions set out in section 94 of the CPPA are met.

It therefore appears that a complainant or organization is unable to apply to the Tribunal without first going through the Commissioner.

2.3.3 Composition of the Tribunal (Sections 6 to 12)

The Tribunal consists of three to six full-time members – or a combination of full-time and part-time members – appointed by the Governor in Council on the recommendation of the Minister. At least one of the members must have experience in the field of information and privacy law (section 6).

2.3.4 Chairperson and Vice-Chairperson (Sections 7 to 9)

The Governor in Council must designate a Chairperson from among the full-time members (section 7). The Chairperson has supervision over the Tribunal and directs its work. For example, he is responsible for the distribution of work among the members, the conduct of the work of the Tribunal and the management of its internal affairs (section 8(1)).

The Governor in Council may also designate a Vice-Chairperson responsible for performing the duties of the Chairperson in the event of the latter's absence, incapacity or vacancy (section 8(2)). If the Chairperson and Vice-Chairperson are not able to perform their duties, a member designated by the Minister acts as Chairperson for a period of no more than 90 days. After that period, any renewal requires approval by the Governor in Council (section 9).

2.3.5 Members of the Tribunal (Sections 10 to 12)

The Tribunal Act guarantees the independence and impartiality of administrative decision-makers and provides for measures to allow members to conclude certain ongoing matters despite the expiry of their mandate.

Tribunal members are appointed to hold office during good behaviour for a first time not exceeding five years, unless removed for cause by the Governor in Council (section 10). The Tribunal Act does not specify the conditions for removal for cause.

The mandate of Tribunal members can be renewed for one or more term not exceeding three years (section 10(2)). A member whose appointment has expired can be given up to six additional months of his or her term at the request of the Chairperson. During those six months, the member is deemed to be a part-time member of the Tribunal and can make or take part in a decision on a matter that they heard as a member (section 10(3)).

Tribunal members receive remuneration fixed by the Governor in Council and are entitled to travel and living expenses associated with their duties. Full-time members are paid travel and living expenses when their duties must be carried out away from their ordinary place of work, while part-time members are paid expenses when their duties are carried out away from their ordinary place of residence. Members may also receive specific compensation for illness, injury or accident as government employees or employees in the federal public administration. Only full-time members of the Tribunal are employees in the public service for the purposes of the *Public Service Superannuation Act*.

A member who holds a pecuniary or other interest in a current matter that could be inconsistent with the proper performance of their duties cannot hear the matter, alone or as a member of a panel. The member must inform the Tribunal's Chairperson of the situation without delay (section 12).

2.3.6 Tribunal Hearings and Decisions (Sections 13 to 21)

2.3.6.1 Principal Office and Sittings (Sections 13 to 14)

The Tribunal Act provides that the principal office of the Tribunal is designated by the Governor in Council and, if no place is designated, is to be in the National Capital Region (section 13). The dates, times and manner in which the Tribunal sits shall be designated by its Chairperson (section 14).

2.3.6.2 Hearings and Rules of Evidence (Section 15)

The Tribunal is not bound by the formal technical rules of evidence to allow for more flexible administration of evidence. In particular, the Tribunal relies on fairness and natural justice to act expeditiously, freely and informally insofar as the circumstances of the hearing permit. The burden of proof is assessed by the Tribunal on the balance of probabilities. However, the Tribunal must not receive or accept any evidence that would normally be inadmissible in a court of law. The parties may choose to represent themselves before the Tribunal or appoint a representative as legal counsel.

2.3.6.3 Proceedings, Decisions and Reasons (Sections 16 to 21)

The Tribunal and its members have the same investigative powers as commissioners appointed under Part I of the *Inquiries Act* and may make interim decisions. They may summon and compel witnesses to appear before the Tribunal verbally or in writing or require that documents be produced when deemed necessary for the inquiry (section 16).

The Tribunal must provide its decisions in writing, with reasons, to all parties to a proceeding. The Tribunal must make its decisions and reasons publicly available while ensuring the privacy of any complainant who has not consented to disclosure of any information that could identify him or her (sections 17 and 18).

The Tribunal may establish its own procedural rules in accordance with the Tribunal Act and the CPPA, and with the approval of the Governor in Council. More specifically, the Tribunal can make its own rules respecting when decisions are to be made public and the factors to be considered in deciding whether to name an organization affected by a decision. The Tribunal must make its procedural rules publicly available (section 19).

The Tribunal may award costs, at its discretion, in accordance with its rules (section 20).[30]

Decisions of the Tribunal are final and binding. They are not subject to appeal or review by any court, except for judicial review under the *Federal Courts Act* (section 21).

NOTES

1. Bill C-11, An Act to enact the Consumer Privacy Protection Act and the Personal Information and Data Protection Tribunal Act and to make consequential and related amendments to other Acts, 43rd Parliament, 2nd Session. A Charter Statement was tabled in the House of Commons on 2 December 2020 by the Department of Justice.
2. For a more comprehensive history of the *Personal Information Protection and Electronic Documents Act* (PIPEDA) and calls for reform over the last 20 years, see Alexandra Savoie and Maxime-Olivier Thibodeau, *Canada's Federal Privacy Laws*, Publication no. 2007-44-E, Library of Parliament, 17 November 2020.
3. Innovation, Science and Economic Development (ISED), *Canada's Digital Charter: Trust in a digital world*. The Charter is a plan that illustrates how the government plans to establish the trust on which the digital and data-driven economy will be built. It is not a legally binding legislative instrument but rather a set of principles that the government will take into account in developing future policies, programs and legislation related to the digital economy.
4. ISED, *Canada's Digital Charter in Action: A Plan by Canadians, for Canadians*.
5. ISED, *Strengthening Privacy for the Digital Age*.
6. Office of the Privacy Commissioner of Canada (OPC), *2018–2019 Annual Report – Privacy Law Reform: A Pathway to Respecting Rights and Restoring Trust in Government and the Digital Economy*, 2018–2019 Annual Report to Parliament on the *Privacy Act* and the *Personal Information Protection and Electronic Documents Act*. The concept of privacy by design refers to consideration of privacy from the early phase of conception of a product or service through to its execution, deployment and beyond, such as an assessment of factors related to privacy.
7. OPC, *Privacy in a pandemic*, 2019–2020 Annual Report to Parliament on the *Privacy Act* and *Personal Information Protection and Electronic Documents Act*.
8. OPC, *Commissioner issues proposals on regulating artificial intelligence*, News release, 12 November 2020; and OPC, *A Regulatory Framework for AI: Recommendations for PIPEDA Reform*, November 2020.
9. House of Commons, Standing Committee on Access to Information, Privacy and Ethics (ETHI), *Towards Privacy by Design: Review of the* Personal Information Protection and Electronic Documents Act, Twelfth report, February 2018.
10. ETHI, *Addressing Digital Privacy Vulnerabilities and Potential Threats to Canada's Democratic Electoral Process*, Sixteenth report, June 2018; and ETHI, *Democracy Under Threat: Risks and Solutions in the Era of Disinformation and Data Monopoly*, Seventeenth report, December 2018.
11. EUR-Lex, *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)* (GDPR), art. 45.
12. EUR-Lex, *Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data*; and Government of Canada, "The European Union's General Data Protection Regulation," *Export guides and statistics*.
13. EUR-Lex, GDPR, art. 45, para. 9.
14. European Commission, *Adequacy decisions*.
15. Government of Canada, *Sixth Update Report on Developments in Data Protection Law in Canada*, Report to the European Commission, December 2019.
16. EUR-Lex, GDPR, art. 45, para. 3.

17. See, for example, *Johnson v. Bell Canada*, 2008 FC 1086 (CanLII), para. 21; and *Fahmy v. Bank of Montreal*, 2016 FC 479 (CanLII), para. 49.

18. To see where the principles from Schedule 1 of PIPEDA were integrated into the CPPA and what provisions of PIPEDA were included in whole or in part in the CPPA, see Teresa Scassa, "Comparison Chart for Bill C-11's CPPA and PIPEDA," *Scholars Portal Dataverse*, 2020.

19. OPC, *Statement from the Privacy Commissioner of Canada following the tabling of Bill C-11*, 19 November 2020.

20. At this time, Alberta, British Columbia and Quebec have enacted legislation that is substantially similar to PIPEDA. In those provinces, PIPEDA does not apply except to the commercial activities of federally governed businesses (as defined in the Act). Note that the French term used in the CPPA is "essentiellement semblable" while the French term used in PIPEDA is "essentiellement similaire." The English term in both is "substantially similar."

21. PIPEDA does not include a provision related to the extraterritorial application of the Act, but the Federal Court decision in *A.T. v. Globe24h.com* affirmed that it can apply abroad when there is a real and substantial link between the cross-border activities of an organization and Canada. The same reasoning should apply to the CPPA.

22. The provisions related to the accountability of organizations in sections 7 to 11 of the CPPA reflect the content of the Principle 1 in Schedule 1 of PIPEDA.

23. Sections 12 to 14 of the CPPA reflect the content of Principle 2, Principle 4 and Principle 5 in Schedule 1 of PIPEDA.

24. Sections 53 to 56 of the CPPA reflect the content of Principle 5 and Principle 6 in Schedule 1 of PIPEDA concerning the limitations applicable to the use, disclosure, retention and accuracy of personal information.

25. The obligation set out in section 57 reflects the content of the Principle 7 in Schedule 1 of PIPEDA concerning security safeguards.

26. Section 62 reflects the content of the Principle 8 in Schedule 1 of PIPEDA concerning openness.

27. Sections 63 to 71 reflect the content of the Principle 9 in Schedule 1 of PIPEDA concerning access to personal information.

28. Sections 82 to 87 reflect the content of the Principle 10 in Schedule 1 of PIPEDA.

29. Sections 13, 14(1), 15(5), 16, 53, 55(1), 55(3), 57(1), 58(1) and 58(3) of the CPPA.

30. Costs are expenses that the winning party can be paid by the other party. See, for example, Department of Justice, *Frais de justice : dépens et autres frais* [AVAILABLE IN FRENCH ONLY].