LIBRARY OF PARLIAMENT
BIBLIOTHÈQUE DU PARLEMENT

Legislative Summary

BILL C-27:
AN ACT TO ENACT THE CONSUMER PRIVACY PROTECTION ACT, THE PERSONAL INFORMATION AND DATA PROTECTION TRIBUNAL ACT AND THE ARTIFICIAL INTELLIGENCE AND DATA ACT AND TO MAKE CONSEQUENTIAL AND RELATED AMENDMENTS TO OTHER ACTS

Publication No. 44-1-C27-E

12 July 2022

Sabrina Charland, Alexandra Savoie and Ryan van den Berg

Parliamentary Information, Education and Research Services

AUTHORSHIP

12 July 2022	Sabrina Charland	Economics, Resources and International 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 Parliamentary Information, Education and Research Services, 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-27
(Legislative Summary)

Publication No. 44-1-C27-E

Ce document est également publié en français.

CONTENTS

LEGISLATIVE SUMMARY OF BILL C-27: AN ACT TO ENACT THE CONSUMER PRIVACY PROTECTION ACT, THE PERSONAL INFORMATION AND DATA PROTECTION TRIBUNAL ACT AND THE ARTIFICIAL INTELLIGENCE AND DATA ACT AND TO MAKE CONSEQUENTIAL AND RELATED AMENDMENTS TO OTHER ACTS

1 BACKGROUND

On 16 June 2022, the Minister of Innovation, Science and Industry introduced in the House of Commons Bill C-27, An Act to enact the Consumer Privacy Protection Act, the Personal Information and Data Protection Tribunal Act and the Artificial Intelligence and Data Act and to make consequential and related amendments to other Acts.[1]

The bill creates three new pieces of legislation: the Consumer Privacy Protection Act (CPPA), the Personal Information and Data Protection Tribunal Act (Tribunal Act) and the Artificial Intelligence and Data Act (AI Act). It repeals Part 1 of the *Personal Information Protection and Electronic Documents Act* (PIPEDA) and changes the short title to the Electronic Documents Act.

Bill C-27 incorporates the content 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, introduced in the House of Commons on 17 November 2020 by the Minister of Innovation, Science and Industry.[2]

Bill C-11, which was the first bill seeking to fully reform the federal legislation on privacy in the private sector since PIPEDA was adopted in 2000, died on the *Order Paper* when Parliament was dissolved in August 2021.[3] The current bill – which makes some amendments to Bill C-11 and also enacts the AI Act – is a new attempt at reform.

In general, the CPPA:

- codifies the contents of the fair information principles set out in Schedule 1 of PIPEDA by rewording 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 the requirement for 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);
- incorporates the concept of algorithmic transparency in the form of a right to an explanation concerning decisions made by an automated decision system (sections 62 and 63);
- incorporates the concept of data portability by allowing two organizations to disclose personal information between them under a data mobility framework (section 72);
- sets out obligations regarding 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 that is the higher of $10,000,000 and 3% of an organization's gross global revenue (sections 93 to 95); and
- provides for a maximum fine not exceeding the higher of $25,000,000 and 5% of an organization's gross global revenue in the case of a conviction for contravening certain specific provisions of the CPPA or in the case of obstructing the Commissioner's work (section 128).

As for the Tribunal Act, it establishes the Personal Information and Data Protection Tribunal (the Tribunal) and defines the internal operation and principles on which its proceedings are founded.

The AI Act regulates international and interprovincial trade and commerce in artificial intelligence systems by establishing requirements for designing, developing and using AI systems and by prohibiting certain behaviours.

In general, the AI Act:

- requires a person who is responsible for a high-impact artificial intelligence system to fulfill certain obligations, including establishing measures related to risks to identify, assess and mitigate the risks of harm or biased output that could result from the use of the system (sections 6 to 12);
- allows the appropriate minister to make orders, including orders to require that an organization subject to the AI Act cease using or making available a high-impact artificial intelligence system if the Minister has reasonable grounds to believe that this system gives rise to a serious risk of imminent harm (sections 13 to 21);

- provides for significant administrative monetary penalties for a violation of the Act and a fine or term of imprisonment for offences under the Act (sections 29, 30 and 38 to 40); and
- allows the appropriate minister to designate the Artificial Intelligence and Data Commissioner to support the minister in the administration and enforcement of Part 1 of the AI Act (section 33).

1.1 CANADA'S DIGITAL CHARTER

The short title of the bill is the Digital Charter Implementation Act, 2022. Canada's Digital Charter (the Digital Charter) was unveiled by Innovation, Science and Economic Development Canada (ISED) in 2019.[4] This charter is the result of consultations that began in June 2018 with many stakeholders.[5] The 10 principles set out in the Digital 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 by adopting regulations that support the principles set out in the Digital Charter.

After releasing the Digital Charter, ISED issued a discussion paper on PIPEDA reform, outlining issues and possible legislative amendments.[6]

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

Bill C-27 responds to 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 on privacy law reform, the Commissioner recommended the modernization of federal privacy laws, including PIPEDA. Among other things, he recommended a rights-based approach for protecting the privacy of Canadians, proactive inspection powers without grounds and privacy by design obligations.[7]

In his 2019–2020 annual report on privacy in a pandemic, the Commissioner reasserted the need to reform federal privacy laws, including PIPEDA. He noted that "[t]he law is simply not up to protecting our rights in a digital environment."[8] In 2020, he made proposals for regulating artificial intelligence, including suggestions for amending PIPEDA.[9]

In his 2020–2021 annual report, the Commissioner reasserted the need to reform federal privacy laws, including PIPEDA. He said he wished he could have stated in his report that Canada had been able to put "contemporary privacy laws fit for the digital age firmly in place to adequately protect Canadians," but that this goal had not yet been achieved.[10]

The Committee has recommended a number of amendments to be made to PIPEDA in recent years, including in its 2018 report on the review of PIPEDA.[11] Numerous recommendations for modernizing PIPEDA were also made in the two reports the Committee published in 2018 as part of its study of the breach of personal information involving Cambridge Analytica and Facebook.[12] Another report by the Committee, written in the context of its study on the collection and use of mobility data by the Government of Canada and published in 2022, contains certain recommendations on the modernization of PIPEDA.[13]

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

Bill C-27 also appears to partially address some of the recommendations that the Office of the Privacy Commissioner of Canada (OPC) made in the submission on Bill C-11 that it presented to the Committee in May 2021.[14]

1.3 ADEQUACY STATUS WITH THE EUROPEAN UNION

Under the *General Data Protection Regulation* (GDPR) of the European Union (EU), 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.[15]

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.[16]

The GDPR replaces that directive. It came into effect on 25 May 2018 and provides for the continuity of existing EU adequacy decisions until they are reassessed.[17] Canada, therefore, maintains its adequacy status for the moment. However, the EU must soon reassess the adequacy of the federal legislation on privacy in the private sector against the GDPR.

The adequacy status ensures that data processed in accordance with the GDPR can be transferred from the EU to Canada, or vice versa, without requiring additional data protection guarantees (e.g., a contractual agreement).[18]

Since 2016, the EC is required to monitor the development 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.[19] The exact date of the reassessment of Canada's adequacy status is not known, but the GDPR provides for a reassessment every four years, which would mean that it should take place no later than 2022.[20]

Because the EC has not yet reassessed Canada's adequacy status, Canada maintains its existing adequacy status.

Of note, the EU recently published a proposal for the regulation of artificial intelligence (AI), which lays down a uniform legal framework for the development, marketing and use of AI. The European proposal sets rules using a risk-based approach. It prohibits AI systems that create an unacceptable risk and imposes legal requirements for high-risk AI systems (e.g., transparency and human oversight).[21] The Government of Canada appears to have chosen a risk-based approach in the AI Act as well.

2 DESCRIPTION AND ANALYSIS

Bill C-27 contains 40 clauses and is divided into four parts:

- Part 1 contains the full text of the new CPPA, the consequential and related amendments, terminology changes, transitional provisions and coordinating amendments.
- Part 2 contains the text of the Tribunal Act and a related amendment.
- Part 3 contains the full text of the AI Act.
- Part 4 contains the coming into force provision for the bill.

The following describes selected aspects of the bill; it does not review all of its provisions or those of the three Acts created by Bill C-27.

2.1 PREAMBLE

The bill includes a preamble that outlines its objectives and intended purpose. It recognizes the need to modernize Canada's legislative framework so that it is suited to the digital age.

The preamble recognizes that "the protection of the privacy interests of individuals with respect to their personal information is essential to individual autonomy and dignity and to the full enjoyment of fundamental rights and freedoms in Canada." It also indicates that the bill "aims to support the Government of Canada's efforts … to establish a regulatory framework that supports and protects Canadian norms and values, including the right to privacy."

The preamble also refers to commercial interests. For instance, it recognizes that the growth of Canada's economy depends on trust in the digital and data-driven economy. It further specifies that organizations of all sizes operate in this economy and "an agile regulatory framework is necessary to facilitate compliance with rules by, and promote innovation within, those organizations."

However, this preamble is not included in the text of the CPPA. It will not appear at the beginning of the CPPA once it is adopted.[22] The first recommendation made in the OPC's submission on Bill C-11 was to add a preamble to the CPPA that would recognize various points, including the right to privacy as a human right.[23]

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

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

Part 1 of the CPPA deals with organizations' obligations as they relate 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 129). Part 3 addresses the coming into force of the provisions of the bill (section 130).

The CPPA reiterates several elements of PIPEDA, but in a structure akin to standard legislative text. The wording in PIPEDA refers to fair information principles in Schedule 1 (the principles set out in Schedule 1 of PIPEDA). These principles are not worded using conventional legislative language.[24] In the CPPA, these principles are incorporated into the text of the Act, using conventional legislative wording.

The CPPA imposes numerous obligations on the organizations 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 below.

2.2.1 Authorized Representatives (Section 4 of the CPPA)

The CPPA states that the rights and recourses provided under the Act may be exercised by a parent, guardian or tutor on behalf of a minor who is not able or does not want to personally exercise those rights and recourses, by a person authorized by law to administer the affairs or property of an individual under a legal incapacity (other than a minor), or by a person authorized by law to administer the estate or succession of a deceased individual. There is no such provision in PIPEDA.

2.2.2 Purpose (Section 5 of the CPPA)

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

The purpose of Bill C-27 is fundamentally the same as that of its predecessor. In his statement concerning the tabling of Bill C-11, 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.[25]

The OPC's submission on Bill C-11 reiterated the Commissioner's comments:

> There is no dispute that the CPPA should both promote rights and commercial interests. The question is what weight to give to each.
>
> In my view, it would be normal and fair for commercial activities to be permitted within a rights framework, rather than placing rights and commercial interests on the same footing.[26]

Although the purpose of the CPPA remains essentially the same as that of PIPEDA, the context in which these rules governing the protection of personal information are established has nevertheless 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).

2.2.3 Application (Section 6 of the CPPA)

The application of the CPPA is the same as that of PIPEDA. The CPPA applies to every organization in respect of personal information that it collects, uses or discloses in the course of commercial activities. It also applies to personal information "about an employee of, or an applicant for employment with, the organization and that organization collects, uses or discloses in connection with the operation of a federal work, undertaking or business" (section 6(1)). In other words, it also applies to the personal information of employees of federally regulated private businesses (e.g., banks and telecommunications companies).[27]

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

The CPPA states that it also applies in respect of personal information that is collected, used or disclosed interprovincially or internationally by an organization, except if the organization is exempt from the application of the CPPA under section 122(2)(b), within a province (section 6(2)). Furthermore, section 122(2)(b) sets out the process by which a province may have its provincial legislation recognized as "substantially similar" to the CPPA.[28]

The CPPA also states that it does not apply in respect of personal information that has been anonymized (section 6(5)). The term "anonymize" is defined as follows in section 2 of the CPPA:

> to irreversibly and permanently modify personal information, in accordance with generally accepted best practices, to ensure that no individual can be identified from the information, whether directly or indirectly, by any means.

Therefore, anonymized data is no longer considered personal information for the purposes of the Act. The CPPA makes a distinction between anonymized information and de-identified personal information (see section 2.2.7 of this Legislative Summary, which covers exceptions to the requirement for consent).

The CPPA does not contain any explicit provisions concerning its extraterritorial application to organizations that do not operate in Canada.[29]

2.2.4 Accountability of Organizations (Sections 7 to 11 of the CPPA)

Under the CPPA, all organizations are accountable for personal information under their control.[30] 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 retains this accountability, even if a service provider carries out the

activities on its behalf. The obligations set out in the CPPA do not apply to a service provider in terms of the information transferred to it by an organization (unless it collects, uses or discloses it for purposes other than those for which the information was transferred to the organization). The organization also ensures that all service providers to which it transfers personal information provide the same protection that it provides under the CPPA itself (sections 7 and 11).

Each organization designates at least one individual to be responsible for matters related to the organization's obligations under the CPPA and implements and maintains a privacy management program (the program). This program covers the policies, practices and procedures the organization has put in place to fulfill its obligations under the CPPA. It takes into account the volume and sensitivity of the personal information under the control of the organization (sections 8 and 9). For example, the personal information of minors is always considered to be sensitive information (section 2(2)).

The organization also gives the Commissioner access to the program, when requested. The Commissioner may, after reviewing the program, provide guidance or recommend that corrective measures be taken by the organization (section 10).

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

Sections 12 to 14 of the CPPA apply a necessity and proportionality test for the collection, use and disclosure of personal information.[31]

The CPPA states that an organization can collect, use or disclose personal information "only in a manner and for purposes that a reasonable person would consider appropriate in the circumstances" (section 12(1)). It lists the factors to consider in determining whether the manner and purposes of collecting, using or disclosing personal information are appropriate. These factors are:

- the sensitivity of the personal information;
- whether the purposes represent legitimate business needs of the organization;
- 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 these purposes must be recorded (section 12(3)). The CPPA does not specify how they are to be recorded.

The organization may collect, use or disclose only the 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).

2.2.6 Consent
(Sections 15 to 17 of the CPPA)

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, and they are summarized in section 2.2.7, below.

Under the CPPA, consent is valid only if the organization provides certain information to the individual concerned. This information must be provided in plain language that an individual to whom the organization's activities are directed would reasonably be expected to understand (sections 15(3) and 15(4)). The information that must be provided is as follows:

- 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 comparison, section 6.1 of PIPEDA provides that consent

> is only valid if it is reasonable to expect that an individual to whom the organization's activities are directed would understand the nature, purpose and consequences of the collection, use or disclosure of the personal information to which they are consenting.

Under the CPPA, an organization may determine 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(5)). Furthermore, 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, a federal or provincial law, or a "reasonable" contract (section 17).

2.2.7 Exceptions to Requirement for Consent (Sections 18 to 52 of the CPPA)

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 contain essentially the same content as in sections 7 and 7.2 to 7.4 and sections 10.2(3) and 10.2(4) of PIPEDA. The new exceptions set out in the CPPA are examined below.

A new exception to consent related to "business activities" allows an organization to collect or use personal information about an individual without their knowledge or consent, if the collection or use is made for a business activity (section 18(1)). The collection or use must meet two conditions:

- a reasonable person would expect the collection or use for such a business activity; and
- the personal information is not collected or used for the purpose of influencing the individual's behaviour or decisions.

The business activities covered by this exception include the organization's activities that are necessary to provide a product or service requested by an individual, as well as activities that are necessary "for the organization's information, system or network security" or "for the safety of a product or service that the organization provides" (section 18(2)).

The organization may also collect or use an individual's personal information without their knowledge or consent if the collection or use is made for the purpose of an activity in which the organization has a "legitimate interest that outweighs any potential adverse effect on the individual resulting from that collection or use" (section 18(3)).

To benefit from the exception to consent for legitimate interest, the organization must meet the two conditions listed in section 18(1) and comply with all other prescribed requirements. It must also assess any potential adverse effect on the individual

concerned that is likely to result from the collection or use of personal information and take reasonable measures to reduce the likelihood that those effects will occur and to mitigate or eliminate them (section 18(4)). The assessment must be recorded in writing and a copy must be provided to the Commissioner on request (section 18(5)).

Under the CPPA, an organization may also transfer an individual's personal information to a service provider without the individual's 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). In section 2 of the CPPA, "de-identify" is defined as follows:

> to modify personal information so that an individual cannot be directly identified from it, though a risk of the individual being identified remains.

An organization may use de-identified information for internal research, analysis and development purposes without the individual's knowledge or consent (section 21).

An organization may also use or disclose personal information without consent as part of a prospective business transaction. However, under the CPPA, that information must be de-identified and it must be necessary to determine whether the transaction will take place. The organization receiving the personal information must also commit, in an agreement between the two organizations that will be party to a potential business transaction, to disclose the information only for the purposes of the transaction and to protect it by security safeguards proportionate to the sensitivity of the information. If the transaction does not take place, the organization receiving the personal information agrees to return it to the organization that disclosed it or to dispose of it within a reasonable time (section 22).

Yet, an organization is not required to de-identify personal information before disclosing it as part of a transaction if it would undermine the objectives of the transaction and if the organization has taken into account the risk of harm to the individual that could result from using or disclosing the information (section 22(2)).

The CPPA also provides 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 in Canada), an organization mandated under a federal or provincial law, or by a prescribed entity to carry out a socially beneficial purpose; and
- the disclosure is made for a socially beneficial purpose.

For the purposes of the CPPA, other than sections 20, 21, 22(1) and 39(1) described above, and sections 55, 56, 63(1), 71, 72, 74, 75 and 116 described below, personal information that has been de-identified is considered personal information (section 2(3)).

2.2.8 Retention, Disposal and Accuracy of Personal Information (Sections 53 to 56 of the CPPA)

Sections 53 to 56 of the CPPA cover the limitations that apply to the period for the retention of personal information and the accuracy of this information:[32]

- Taking into account the sensitive nature of personal information when establishing the period for retention, the organization can retain the information only for the time needed to fulfill the purposes for which the information was collected, used or disclosed, or to comply with the requirements of the Act, federal or provincial law or any reasonable terms of a contract (section 53);
- An organization that uses personal information to make a decision about an individual 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 the possibility that the information is used to make a decision about the individual, the fact that the information is used on an ongoing basis, and the fact that the information is disclosed to third parties (section 56).

The CPPA introduces a new explicit right of disposal of personal information (section 55), which represents a form of the right to erasure. Disposal involves permanently and irreversibly deleting personal information or anonymizing it.[33]

At an individual's request, and as soon as possible, the organization proceeds with the disposal of their personal information that is under the organization's control. An organization may refuse a request to dispose of personal information in the following circumstances, even if an individual has withdrawn their consent, in whole or in part, or if the information is no longer necessary for the continued provision of a product or service:

- disposing of their information would result in the disposal of personal information about another individual and the information is not severable;

- legal requirements or reasonable terms of a contract prevent the disposal;
- the information is necessary for the establishment of a legal defence or in the exercise of other legal remedies;
- the information is not in relation to a minor and the disposal of the information would have an undue adverse impact on the accuracy or integrity of information that is necessary to the ongoing provision of a product or service;
- the request is vexatious or made in bad faith; or
- the information (not in relation to a minor) is already scheduled to be disposed of in accordance with the organization's information retention policy, and the organization informs the individual of the remaining period of time for which the information will be retained.

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 must notify the individual of their right to file a complaint with the organization or the Commissioner. If the organization disposes of an individual's personal information, it must also notify all service providers to which the information was transferred that a request for disposal has been made, and ensure that the service provider has disposed of the information (section 55).

2.2.9 Security Safeguards (Sections 57 to 61 of the CPPA)

Under the CPPA, an organization must protect the personal information that it holds[34] 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 storage method of the information (section 57).

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

The system requires an organization to report to the Commissioner any breach of security safeguards concerning 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 can happen in various forms, for example bodily harm, humiliation, damage to reputation or relationships, or financial loss (section 58(7)).

An organization that notifies an individual of a breach of security safeguards that concern them 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 keeps a record of breaches of security safeguards involving personal information and gives the Commissioner access to the record upon request (section 60). Where a service provider determines that a breach of security safeguards involving personal information has occurred, it must, as soon as feasible, notify the organization that controls the personal information (section 61).

2.2.10 Openness and Transparency (Section 62 of the CPPA)

The CPPA requires that an organization make readily available information explaining its policies and practices aimed at complying with the Act.[35] The information that an organization must make accessible includes:

- a general account of how the organization uses the personal information and of how it applies the exceptions to the requirement to obtain an individual's consent, including a description of any activities in which it has a legitimate interest;
- whether it carries out any international or interprovincial transfer or disclosure of personal information that may have reasonably foreseeable privacy implications;
- a general account of its use of automated decision systems to make predictions, recommendations or decisions that could have a significant impact on individuals; and
- the retention periods applicable to sensitive personal information.

In the second category of information mentioned above, an organization is required to make available information about its cross-border data flows, but only if it has determined that these exchanges may have privacy implications for the individuals involved.

With respect to the third category of information an organization must provide, the term "automated decision system" is defined as follows in section 2 of the CPPA:

> any technology that assists or replaces the judgment of human decision-makers through the use of a rules-based system, regression analysis, predictive analytics, machine learning, deep learning, a neural network or other technique.

Thus, in section 62, the CPPA introduces the concept of algorithmic transparency, in the form of a right to explanation. This right to explanation is also present in section 63 of the CPPA.

2.2.11 Access to and Amendment of Personal Information (Sections 63 to 71 of the CPPA)

Upon request by an individual, an organization indicates 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 an individual, and this prediction, recommendation or decision could have a significant impact on them, that individual may request an explanation from the organization about the prediction, recommendation or decision. The organization must then indicate the type of personal information that was used to make the prediction, recommendation or decision, the source of the information and the reasons or principal factors that led to the prediction, recommendation or decision. The individual makes an access request in writing (sections 63 and 64).[36] The CPPA does not give the individual any explicit right to make submissions to an employee of the organization seeking to have a decision reversed when an automated decision system has been used.

The CPPA requires the organization to provide all the information requested under section 63 (section 66) in plain language, which should prevent the communication of lengthy documents written in complex legal terms.

The organization responds to the information request no later than 30 days after it is received, unless the organization informs the individual, within 30 days following the receipt of the request, that the time limit will be extended (for a maximum of 30 additional days) or that a longer period is needed to convert the personal information into an alternative format. Refusal to comply with the information request must be justified; in this case, the organization explains to the individual the reason for refusal and advises them of any recourse they may have (section 67). The organization may charge a minimal fee for processing a request for information (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 they may have under the CPPA (section 69).

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

If an individual asks an organization to notify them of any disclosure made 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 it has relating to such a disclosure, the organization notifies the government institution involved. Within 30 days of receiving the request, the institution notifies the organization that it does

or does not object to providing the requested information to the individual. The institution can only object in certain circumstances, such as when it is of the opinion that fulfilling the request for information or access could pose a risk to national security or law enforcement (sections 70(3) to 70(5)).

If an institution objects, the organization refuses to fulfill 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 give the individual the name of the government institution it notified, nor does it inform the individual about the institution's objection to the organization fulfilling their 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)):

- 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 another 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 violation of federal or provincial law and collecting it otherwise would have compromised the availability or the accuracy of the information;
- the information was 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 the amendment of personal information, if an individual has been given access to their personal information and demonstrates to an organization that the information 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 a disagreement arises 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).

2.2.12 Mobility of Personal Information (Section 72 of the CPPA)

The CPPA incorporates the concept of data portability into the Act as a right to the mobility of personal information. This right allows an individual to request that the personal information collected from them by one organization be transmitted to another organization chosen by the individual. However, under the CPPA, this transfer is allowed only if both organizations involved are subject to a data mobility framework. Regulations will likely provide further details on the application of this provision.

2.2.13 De-identification of Personal Information (Sections 74 and 75 of the CPPA)

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 the term "technical and administrative measures" (section 74).

The CPPA also prohibits an organization from using de-identified information, alone or in combination with other information, to identify an individual. In other words, it prohibits the re-identification of personal information, except in certain circumstances. These circumstances include primarily testing the following: the effectiveness of the security safeguards the organization has put in place; the effectiveness of its de-identification processes; and the fairness and accuracy of the models, processes and systems developed using de-identified information (section 75).

2.2.14 Codes of Practice and Certification Programs (Sections 76 to 81 of the CPPA)

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 is 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 this 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).

2.2.15 Investigation of Complaints, Inquiries, Penalties and Appeals (Sections 82 to 95 and 100 to 106 of the CPPA)

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.[37]

PIPEDA outlines reasons that a complaint is inadmissible (section 12(1) of PIPEDA) and reasons for the discontinuance of an investigation (section 12.2(1) of PIPEDA). Under the CPPA, these reasons are grouped together and can be used by the Commissioner to justify the inadmissibility of a complaint or to discontinue the investigation of a complaint (sections 83(1) and 85). The Commissioner may reconsider a decision not to investigate if satisfied that the complainant has established that there are compelling reasons to investigate (section 83(3)).

The CPPA also contains a new ground based on which the Commissioner can refuse to investigate a complaint, 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)).

If the Commissioner discontinues the investigation of a complaint, or if the Commissioner determines upon concluding the investigation that an inquiry will not be conducted, the Commissioner must notify both the complainant and the organization involved in the complaint and give reasons for the decision (sections 83(2) and 88). The Commissioner may attempt to resolve a complaint through mediation or conciliation. The Commissioner may also enter into a compliance agreement with an organization to ensure compliance with the CPPA (sections 86 and 87).

The inquiry process under the CPPA replaces sections 14 to 17 of PIPEDA, which provide for the possibility of recourse before the Federal Court following the investigation of a complaint by the Commissioner and the Commissioner's summary report of 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 an inquiry into the complaint will be conducted. The Commissioner can also conduct an inquiry if reasonable grounds exist to believe that a compliance agreement has not been complied with (sections 89 and 90). In an inquiry under the CPPA, the Commissioner

is not bound by the legal or technical rules of evidence. Rather, the Commissioner tries to deal with the matter informally and expeditiously and is free to establish the rules regarding the conduct of an inquiry, including the procedure and rules of evidence to be followed. The Commissioner must make those rules public (sections 91 and 92).

Upon completing the inquiry, the Commissioner makes a decision that sets out his findings as to whether the organization contravened the CPPA or failed to comply with a compliance agreement, any order made, or any recommendation to the Tribunal to impose a penalty. The Commissioner also specifies the reasons for his findings, orders or decisions to make recommendations (section 93).

Under section 93(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 the CPPA;
- comply with the terms of a compliance agreement to which it is a party; 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 as the result of an appeal) may be made an order of the Federal Court for the purpose of its enforcement (sections 104 to 106).

The CPPA does not give the Commissioner the power to impose a penalty. Only the Tribunal can impose a penalty by recommendation of the Commissioner or of its own initiative as the result of an appeal, if the Commissioner has not made any such recommendation.

The Commissioner recommends a penalty if it is determined that an organization has contravened one or more specific provisions of the CPPA.[38] The Commissioner must consider certain factors, including the nature and scope of the violation, any evidence that the organization exercised due diligence to avoid the contravention, whether the organization made reasonable efforts to mitigate or reverse the contravention's effects, and the organization's history of compliance with the CPPA. The Commissioner cannot recommend a penalty if it is determined that, at the time of the violation of a CPPA provision, the organization was compliant with the requirements of an approved certification program in relation to that provision (section 94).

Any decision, finding or order by the Commissioner can be appealed to the Tribunal, which may dismiss the appeal or allow it, and in allowing the appeal, substitute its own finding, order or decision for the one under appeal. The standard of review for an appeal is set out in the CPPA (sections 101 to 103).

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 101(1) of the CPPA, it determines 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 findings, if it substitutes them for those of the Commissioner in an appeal) (sections 95(1) and 95(2)). A penalty cannot be imposed on an organization for contravening the CPPA if a prosecution for the act or omission that constitutes the contravention has been instituted against the organization, or if the organization establishes that it exercised due diligence to prevent a violation of the CPPA (section 95(3)).

The maximum penalty for all violations 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 95(4)). To determine the amount of the penalty, the Tribunal must consider the following points (section 95(5)):

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

The CPPA states that the purpose of a penalty is not to punish, but to promote compliance with this Act (section 95(6)).

2.2.16 Audits
(Sections 97 and 98 of the CPPA)

The Commissioner may, with reasonable notice, audit the personal information management practices of an organization if the Commissioner has reasonable grounds to believe that the organization has contravened, is contravening or is likely to contravene Part 1 of the CPPA (section 97). After the audit, the Commissioner presents his findings and recommendations considered appropriate to the organization (section 98).

2.2.17 Commissioner's Powers, Duties and Functions (Sections 99 and 109 to 119 of the CPPA)

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 the Commissioner 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 to investigate a complaint, or to conduct an inquiry or audit (section 99).

In addition, in carrying out the Commissioner's duties and functions, the Commissioner takes into account the purpose of the Act, the organization's size and revenues, the volume and sensitivity of the personal information under the organization's control, as well as matters of general public interest (section 109).

The Commissioner retains the mandate of promoting the purpose of the CPPA and can now also advise an organization on its privacy management program or recommend corrective measures in relation to the program (section 110(1)). The Commissioner must not use the policies, practices and procedures in an organization's program as grounds to initiate a complaint or to carry out an audit unless the Commissioner considers that the organization is willfully disregarding the corrective measures that were recommended in relation to its privacy management program (section 111). The Commissioner must also make public information about how they exercise the duties and functions entrusted to them under the CPPA (section 112).

Under section 113, the Commissioner and persons acting on the Commissioner's behalf or under the Commissioner's direction must not disclose any information they receive in carrying out almost all of their duties and functions set out in the CPPA (sections 113(1) and 113(2)). However, the Commissioner may make public any information learned in the exercise of his powers or the performance of his duties or functions under the Act, if he considers it in the public interest to do so (section 113(3)). The Commissioner may also disclose – or authorize the persons acting on the Commissioner's behalf or under the Commissioner's direction to disclose – information, for instance in the course of a proceeding or an appeal before the Tribunal or a judicial review (sections 113(4), 113(5), 113(7) and 113(8)). If the Commissioner is of the opinion that evidence exists of the commission of offences under federal or provincial law by an officer or employee of an organization, the Commissioner may disclose to the Attorney General of Canada or of a province information relating to the commission of an offence (section 113(6)).

The Commissioner and persons acting on behalf or under the direction of the Commissioner may be called to testify on matters that come to their knowledge as a result of exercising the Commissioner's duties or functions under the CPPA, but only in three circumstances: as part of the prosecution for an offence under section 128 of the CPPA; as part of the prosecution for an offence under the *Criminal Code* (perjury) concerning a statement made under the CPPA; or as part of a proceeding or an appeal before the Tribunal (section 114).

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 while exercising their duties. They also have immunity from defamation proceedings (section 115).

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 research on issues of mutual interest and publish the findings (section 118). The Commissioner may consult with provincial counterparts to ensure that the protection of personal information is as consistent as possible and to enter into agreements or arrangements with them, particularly to coordinate the activities of their respective offices by providing mechanisms to handle any complaint in which they both have an interest. Under the procedure set out in the agreement or arrangement, the Commissioner can also provide information that may be of use to the Commissioner's counterparts or assist them as they carry out their duties and functions to protect personal information (section 119).

The Commissioner may also disclose some information to a person or organization that, under foreign legislation, has powers, duties and functions similar to those of the Commissioner, or is responsible for suppressing conduct similar to that which contravenes the CPPA. Information can only be disclosed if the two parties have entered into a written agreement (section 120).

The Commissioner tables, in each house of Parliament, an annual report on the application of the CPPA, on the extent to which the provinces enacted substantially similar legislation and on the application of any such provincial legislation (section 121).

2.2.18 Private Right of Action (Section 107 of the CPPA)

The CPPA introduces a private right of action that gives a cause of action for damages to an individual affected by the acts or omissions of an organization that has contravened the CPPA. Action can only be brought if the Commissioner or the Tribunal finds that the organization has contravened the CPPA or if the organization is fined for a contravention of the CPPA under section 128. A limitation period of two years applies to this private right of action.

2.2.19 Fines
(Section 128 of the CPPA)

Section 128 provides that any organization that contravenes certain specific provisions of the CPPA (sections 58, 60(1), 69, 75 and 127(1)) or an order made by the Commissioner, or that obstructs the work of the Commissioner's office during an audit, an inquiry or an investigation of a complaint, 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 earned 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 considerable increase in the fines set out in section 28 of PIPEDA, where the maximum fine for an offence under that Act was $100,000.

Unlike the administrative penalty provided for in section 95 of the CPPA, the fines under section 128 are not imposed by the Tribunal. Rather, they are imposed by a court following prosecution for an offence, at the discretion of the Attorney General of Canada.

2.2.20 General Provisions
(Sections 122 to 127 and 129 of the CPPA)

The Governor in Council may make regulations for carrying out the purposes and provisions of the CPPA, for example, to govern the scope of the business activities set out in section 18 (section 122(1)(a)). The Governor in Council may also, by order, provide for certain things, particularly, which organizations are exempt from the application of the CPPA when provincial legislation recognized as being substantially similar to CPPA applies (section 122(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 122(3)).

The Governor in Council may also make regulations respecting the data mobility frameworks set out in section 72 and the codes of practice and certification programs set out in sections 76 to 81 of the CPPA (sections 123 and 125). Regulations for applying the CPPA made under section 122(1) or section 123 may distinguish different classes of activities, government institutions and parts of such institutions, information, organizations or entities (section 124).

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 126). 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 violation 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 take one of the actions noted above (section 127).

A parliamentary committee will review the CPPA every five years (section 129).

2.2.21 Coming into Force (Section 130 of the CPPA)

The CPPA comes into force on the day on which clause 3 of the bill, which provides for the replacement of the title of PIPEDA by "An Act to provide for the use of electronic means to communicate or record information or transactions," comes into force.

The following sections of the CPPA come into force on a day to be fixed by order of the Governor in Council:

- sections 72 and 123, which address the data mobility framework;
- sections 76 to 81, which address codes of practice and certification programs;
- sections 83(1)(d) and 94(3), which allow the Commissioner to discontinue the investigation of a complaint if the complaint raises an issue in respect of which a certification program that was approved by the Commissioner applies, or to ensure that a penalty is not recommended if the organization was in compliance with the requirements of a certification program; and
- section 125, which provides that the Minister may make regulations respecting codes of practice and certification programs.

2.3 CONSEQUENTIAL AND RELATED AMENDMENTS, TERMINOLOGICAL AMENDMENTS AND TRANSITIONAL PROVISIONS (CLAUSES 3 TO 36 OF THE BILL)

Bill C-27 makes consequential and related amendments to other Acts. It amends PIPEDA by repealing several parts and replacing its short title with the Electronic Documents Act. The amendment reduces the scope of the Electronic Documents Act to the federal government's use of electronic means to record or communicate information (clauses 3 to 8 of the bill). The content of the repealed parts of PIPEDA is reflected in parts 1 and 2 of the CPPA.

Consequential and related changes are also made to other Acts to make reference to the CPPA and its relevant provisions or to the Tribunal (clauses 9 to 32 of the bill). 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 113(2).
- Section 4.83(1) of the *Aeronautics Act*, which deals with information requests made by foreign states, is amended to replace the reference to PIPEDA with a reference to Part 1 of the CPPA.
- Clauses 14 and 17 of the Schedule to the *Canada Evidence Act* (which contains a numbered list of entities designated for the purposes of other Acts) are amended. References to PIPEDA in clauses 14 and 17 of this Schedule are replaced by references to the CPPA. Clause 17 of this Schedule identifies the Personal Information and Data Protection Tribunal as the designated entity for the purposes of the CPPA, rather than the Federal Court.

The bill 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 establish the procedure for disclosing information to the Privacy Commissioner. It also amends the *Telecommunications Act* to authorize disclosure of designated information to the Privacy Commissioner (clauses 13, 14 and 16 of the bill).

The bill amends a few other Acts to replace any reference to PIPEDA with a reference to the CPPA and its relevant parts or provisions (clauses 15 and 17 to 32 of the bill). The bill also amends terminology in 13 Acts to replace all references to PIPEDA with a reference to the Electronic Documents Act (clause 33 of the bill).

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 section 82 of the CPPA 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 34 of the bill).

2.4 PERSONAL INFORMATION AND DATA PROTECTION TRIBUNAL ACT (CLAUSES 37 AND 38 OF THE BILL)

Part 2 of the bill contains two clauses. The first enacts the Tribunal Act, which creates the Tribunal (clause 37 of the bill). The second provides for a related amendment to the *Administrative Tribunals Support Service of Canada Act* to add the Tribunal to the list of administrative tribunals in the schedule to that Act (clause 38 of the bill).

2.4.1 Introductory Provisions and Definitions (Sections 2 and 3 of the Tribunal Act)

Under the Tribunal Act, the minister responsible for enforcing the Act is 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.

2.4.2 Establishment and Jurisdiction of the Tribunal (Sections 4 and 5 of the Tribunal Act)

Section 4 of the Tribunal Act establishes the Tribunal, with limited jurisdiction. The Tribunal can rule only on appeals made under section 101 or 102 of the CPPA or in respect of penalties imposed under section 95 of that Act (section 5).

The Tribunal hears all appeals from inquiries by the Commissioner, a compliance order issued by the Commissioner to an organization or a decision by the Commissioner not to recommend that a penalty be imposed on an organization that may have contravened the CPPA (section 101 of the CPPA). The Tribunal can also grant leave to appeal an interim order that the Commissioner considers appropriate as part of a complaint, inquiry or audit (section 102 of the CPPA). Lastly, the Tribunal has jurisdiction to impose a penalty on an organization when the conditions set out in section 95 of the CPPA are met.

Thus, it seems impossible for a complainant or organization to address the Tribunal without first going through the Commissioner.

2.4.3 Composition of the Tribunal (Section 6 of the Tribunal Act)

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

2.4.4 Chairperson and Vice-Chairperson (Sections 7 to 9 of the Tribunal Act)

The Governor in Council must designate a full-time member as Chairperson (section 7). The chairperson supervises the Tribunal and directs its work. For example, the chairperson 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 (section 7). The vice-chairperson is responsible for performing the duties of the chairperson in the chairperson's absence or incapacity, or if the position of chairperson becomes vacant (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).

2.4.5 Term and Remuneration of Members of the Tribunal (Sections 10 to 12 of the Tribunal Act)

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

Tribunal members are appointed to hold office during good behaviour for a term 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 term or more, not exceeding three years each (section 10(2)). A member whose appointment has expired can receive a term extension of up to six additional months at the request of the chairperson so that the member can take part in decisions on matters that they heard as a member, in which case the former member is deemed to be a part-time member (section 10(3)).

Tribunal members receive remuneration fixed by the Governor in Council, and they 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* (section 11).

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, either alone or as a member of a panel. The member must inform the Tribunal's chairperson of the situation without delay (section 12).

2.4.6 Tribunal Hearings and Decisions (Sections 13 to 21 of the Tribunal Act)

2.4.6.1 Principal Office and Sittings (Sections 13 and 14 of the Tribunal Act)

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 in the National Capital Region (section 13). The dates, times and manner in which the Tribunal sits are designated by its chairperson (section 14).

2.4.6.2 Hearings and Rules of Evidence (Section 15 of the Tribunal Act)

The Tribunal is not bound by the formal technical rules of evidence at hearings, allowing for the much 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 discharged by proof 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 to appoint a representative, including legal counsel.

2.4.6.3 Proceedings, Decisions and Reasons (Sections 16 to 21 of the Tribunal Act)

The Tribunal has all the powers, rights and privileges that are vested in a superior court of record, with respect to the appearance, swearing and examination of witnesses, the production and inspection of documents, the enforcement of its decisions and other matters necessary or proper for the due exercise of its jurisdiction (section 16(1)).

A Tribunal decision may, for the purposes of its enforcement, be made an order of the Federal Court or of any superior court. These decisions are enforceable in the same manner as an order of the court. To make a decision of the Tribunal an order of a court, either the usual procedure of the court in such matters may be followed or a certified copy of the decision may be filed with the registrar of the court (sections 16(2) and 16(3)).

The Tribunal must provide its decisions in writing, with reasons. The Tribunal ensures that its decisions and reasons are publicly available, while protecting the privacy of any complainant who has not consented to the disclosure of information that could be used to identify them (sections 17 and 18).

The Tribunal may establish its own procedural rules in accordance with the Tribunal Act and the CPPA, with the approval of the Governor in Council. More specifically, the Tribunal can make its own rules about 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 makes the procedural rules it establishes publicly available (section 19).

The Tribunal may award costs,[39] at its discretion, in accordance with its rules (section 20).

The Tribunal's decisions are final and binding. They are not subject to appeal or review by any court, other than judicial review under the *Federal Courts Act* (section 21).

The Tribunal Act does not include any coming into force provisions. Therefore, it comes into force at the time of Royal Assent.

2.5 ARTIFICIAL INTELLIGENCE AND DATA ACT (CLAUSE 39 OF THE BILL)

The AI Act is divided into three parts and has 41 sections. Part 1 of the AI Act addresses the regulation of AI systems in the private sector (sections 5 to 37). Part 2 of the AI Act outlines general offences related to AI systems (sections 38 to 40). Lastly, Part 3 contains the coming into force provision for the AI Act (section 41). The provisions of the AI Act come into force on a day or days to be fixed by order of the Governor in Council.

2.5.1 Application (Section 3 of the AI Act)

The application of the AI Act is limited to the private sector, as part of international and interprovincial trade and commerce associated with artificial intelligence systems (AI systems). Thus, the AI Act does not apply to government institutions as defined in section 3 of the *Privacy Act*, nor with respect to a product, service or activity that is under the direction or control of

- the minister of National Defence;
- the director of the Canadian Security Intelligence Service;

- the chief of the Communications Security Establishment; or
- any other person who is responsible for a federal or provincial department or agency and who is prescribed by regulation.

2.5.2 Purposes of the Act (Section 4 of the AI Act)

The purposes of the AI Act are

- to regulate international and interprovincial trade and commerce in AI systems by establishing common requirements, applicable across Canada, for the design, development and use of those systems; and
- to prohibit certain conduct in relation to AI systems that may result in serious harm to individuals or harm to their interests.

Under section 5(1) of the AI Act, the term "harm" means "physical or psychological harm to an individual, damage to an individual's property or economic loss to an individual." The term "serious harm" is not defined in the AI Act, nor is the term "material harm," even though it is used in section 12. What constitutes "material harm" in section 12 will be determined by regulation (section 36).

2.5.3 Requirements (Sections 6 to 12 of the AI Act)

The requirements set out in the AI Act apply to regulated activities. For the purposes of the AI Act, "processing or making available for use any data relating to human activities for the purpose of designing, developing or using an [AI] system" and "designing, developing or making available for use an [AI] system or managing its operations" in the course of international or interprovincial trade and commerce are considered "regulated activities" (section 5).

A person who carries out any regulated activity and who processes or makes available for use anonymized data must establish measures with respect to the manner in which data is anonymized and the use or management of anonymized data (section 6).[40]

In accordance with the regulations, a person who is responsible for an AI system (the person who designs it, develops it or makes it available for use) must determine whether it is a high-impact system, in other words, whether the AI system meets the criteria for a high-impact system established by regulation. If it does, the person responsible for the AI system must establish measures to identify, assess and mitigate the risks of harm or biased output that could result from the use of the system. They must also establish measures to monitor compliance with the mitigation measures and assess their effectiveness (sections 7 to 9).

The term "biased output" is defined in section 5(1) of the AI Act as

> content that is generated, or a decision, recommendation or prediction that is made, by an artificial intelligence system and that adversely differentiates, directly or indirectly and without justification, in relation to an individual on one or more of the prohibited grounds of discrimination set out in section 3 of the *Canadian Human Rights Act*, or on a combination of such prohibited grounds. It does not include content, or a decision, recommendation or prediction, the purpose and effect of which are to prevent disadvantages that are likely to be suffered by, or to eliminate or reduce disadvantages that are suffered by, any group of individuals when those disadvantages would be based on or related to the prohibited grounds.

A person who carries out any regulated activity must, in accordance with the regulations, keep records describing in general terms the measures relating to the anonymization of data and high-impact systems they establish and the reasons supporting their assessment of whether an AI system is a high-impact system (section 10).

A person who makes available for use a high-impact system or manages the operation of such a system must publish, on a publicly available website, a plain-language description of the system that explains: how the system is intended to be used or is used; the types of content that it is supposed to generate or does generate; and the decisions, recommendations or predictions that it is intended to make or does make. This person must also publish the mitigation measures established with regard to the high-impact AI system and any other information that may be prescribed by regulation (section 11).

Under the AI Act, a person who is responsible for a high-impact system must, as soon as feasible, notify the Minister if the use of the system results or is likely to result in material harm (section 12).

2.5.4 Ministerial Orders (Sections 13 to 21 of the AI Act)

The Minister responsible for the application of the AI Act may, by order, require that a person carrying out a regulated activity provide the Minister with any of the records referred to in section 10 of the AI Act, including where the Minister has reasonable grounds to believe the use of a high-impact AI system could result in harm or biased output (sections 13 and 14).

If the Minister has reasonable grounds to believe that a person has contravened any of sections 6 to 12 or an order made under sections 13 and 14 of the AI Act, the Minister may, by order, require that the person conduct an audit, at their cost, with respect to

the possible contravention or that they engage the services of an independent auditor to conduct the audit. The audit must be conducted by a person who meets the qualifications prescribed by regulations, and the person who is audited must provide the Minister with the audit report (section 15).

The Minister may, by order, require the implementation of any measure specified in the order to address anything referred to in the audit report (section 16). If the Minister has reasonable grounds to believe that the use of a high-impact system gives rise to a serious risk of imminent harm, the Minister may, by order, require that any person who is responsible for that system cease using it or making it available for use (section 17).

The Minister may also, by order, require the publication of information relating to sections 6 to 12 of the AI Act, or to orders made under sections 15 and 16 of the AI Act. However, the Minister is not permitted to require that the person disclose confidential business information (section 18).

The Minister may file in the Federal Court a certified copy of an order made under any of sections 13 to 18 of the AI Act, at which point the order becomes and may be enforced as an order of the Federal Court (section 20).

2.5.5 Information
(Sections 22 to 28 of the AI Act)

The Minister must take measures to maintain the confidentiality of any confidential business information that the Minister obtains under Part 1 of the AI Act. This information does not lose its confidential nature by the mere fact that it is so obtained or that it has been disclosed by the Minister under sections 25 and 26 (sections 22 and 23).

The Minister may disclose confidential business information in certain cases, such as for the purpose of complying with a subpoena or warrant issued or order made by a court. The Minister may also disclose that information that to an analyst designated to oversee the administration and enforcement of Part 1 of the AI Act (sections 24 and 25).

The Minister may also disclose any personal information or confidential business information obtained under Part 1 of the AI Act to any person or entity responsible for administering or enforcing a federal or provincial Act, such as the Privacy Commissioner of Canada and their provincial counterparts (section 26).[41] To do so, the Minister must:

- have reasonable grounds to believe that a person who carries out any regulated activity under the AI Act has contravened, or is likely to contravene, another federal or provincial Act;

- be satisfied that the disclosure is necessary for the purposes of enabling the recipient to administer or enforce the Act in question; and
- ensure that the recipient of the information agrees in writing to maintain the confidentiality of the information.

For the purpose of encouraging compliance with Part 1 of the AI Act, and if the Minister considers that it is in the public interest to do so, the Minister may publish information about any contravention of this Part on a publicly available website. The Minister may also publish information they obtained that relates to an AI system if the Minister has reasonable grounds to believe that the use of the system gives rise to a serious risk of imminent harm, and that the publication of the information is essential to prevent the harm. However, the Minister is not permitted to publish personal information or confidential business information (sections 27 and 28).

2.5.6 Administrative Monetary Penalties (Section 29 of the AI Act)

The Governor in Council may make regulations respecting an administrative monetary penalties scheme. For example, the Governor in Council may make regulations designating the provisions of the Act the contravention of which constitutes a violation, as well as regulations imposing the amount or range of amounts and the factors to be taken into account to determine the administrative monetary penalty. The purpose of an administrative monetary penalty is to encourage compliance with Part 1 of the AI Act and not to punish. If an act or omission is both a violation and an offence, only one proceeding (administrative or criminal) can take place.

2.5.7 Offences (Section 30 of the AI Act)

When a person contravenes any of sections 6 to 12 of the AI Act, they are guilty of an offence. When a person who carries on a regulated activity obstructs or provides false or misleading information to the Minister, anyone acting on behalf of the Minister or an independent auditor, they are guilty of an offence and are liable to a punishment in the form of a fine. The amount of the fine varies based on the type of offence and to whom it applies. The person

> (a) is liable, on conviction on indictment,
>
> > (i) to a fine of not more than the greater of $10,000,000 and 3% of the person's gross global revenues in its financial year before the one in which the person is sentenced, in the case of a person who is not an individual, and

(ii) to a fine at the discretion of the court, in the case of an individual; or

(b) is liable, on summary conviction,

(i) to a fine of not more than the greater of $5,000,000 and 2% of the person's gross global revenues in its financial year before the one in which the person is sentenced, in the case of a person who is not an individual, and

(ii) to a fine of not more than $50,000, in the case of an individual.[42]

The fine is imposed following a criminal procedure before a court.

It is sufficient proof of an offence to establish that it was committed by an employee, agent or mandatary of the accused. However, a person is not to be found guilty of an offence if they establish that they exercised due diligence to prevent the commission of the offence. The accused may also establish that the offence was committed without their knowledge or consent (sections 30(4) and 30(5)).

2.5.8 Administration of the Act (Sections 31 to 37 of the AI Act)

The Minister responsible for the administration of the AI Act is designated by the Governor in Council (section 31). The Minister may promote public awareness of the AI Act and provide education with respect to it, make recommendations and cause to be prepared reports on the establishment of measures to facilitate compliance with Part 1 of this Act, and establish guidelines with respect to compliance with it (section 32). The Minister may designate a senior official, to be called the Artificial Intelligence and Data Commissioner, to whom the Minister may delegate any power, duty or function conferred on the Minister under Part 1 of the AI Act, except the power to make regulations (section 33). The Minister may also designate any individual as an analyst for the administration and enforcement of Part 1 of the AI Act and establish a committee to advise the Minister on any matters related to this Part and cause the advice of this committee to be published (sections 34 and 35).

In addition, the Minister may make regulations respecting, among other things, the records to be kept under section 10 of the AI Act, prescribing the time and the manner in which descriptions are to be published for the purposes of sections 11(1) and 11(2), and respecting the notice of material harm to be provided under section 12 and the publication of information under section 18 (section 37). The other regulations for the purposes of Part 1 are made by the Governor in Council (section 36).

2.5.9 General Offences Related to Artificial Intelligence Systems (Sections 38 to 40 of the AI Act)

A person commits an offence if they are in possession of personal information for the purpose of designing, developing, using or making available for use an AI system, knowing or believing that the information is obtained or derived, directly or indirectly, as a result of the commission of an offence under a federal or provincial act, or as a result of an act or omission outside of Canada that would have constituted such an offence if it had occurred in Canada (section 38).[43]

If a person is without lawful excuse and, knowing that or being reckless as to whether the use of an AI system is likely to cause serious physical or psychological harm to an individual (or substantial damage to an individual's property), makes that AI system available for use, and causes such harm, that person commits an offence. As well, if a person with intent to defraud the public and to cause substantial economic loss to an individual makes an AI system available for use and its use causes that loss, that person commits an offence under the AI Act (section 39).

A person who commits one of the general offences listed above will be liable to a punishment that varies based on the type of offence and to whom it applies. The person:

> (a) is liable, on conviction on indictment,
>
> > (i) to a fine of not more than the greater of $25,000,000 and 5% of the person's gross global revenues in its financial year before the one in which the person is sentenced, in the case of a person who is not an individual, and
> >
> > (ii) to a fine in the discretion of the court or to a term of imprisonment of up to five years less a day, or to both, in the case of an individual; or
>
> (b) is liable, on summary conviction,
>
> > (i) to a fine of not more than the greater of $20,000,000 and 4% of the person's gross global revenues in its financial year before the one in which the person is sentenced, in the case of a person who is not an individual, and
> >
> > (ii) to a fine of not more than $100,000 or to a term of imprisonment of up to two years less a day, or to both, in the case of an individual.[44]

As with the other offences set out in the AI Act, punishment is imposed after a criminal proceeding before the courts.

NOTES

1. Bill C-27, An Act to enact the Consumer Privacy Protection Act, the Personal Information and Data Protection Tribunal Act and the Artificial Intelligence and Data Act and to make consequential and related amendments to other Acts, 44th Parliament, 1st Session. At the time of writing this Legislative Summary, a Charter Statement regarding Bill C-27 had not yet been tabled in the House of Commons.

2. 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. The Department of Justice tabled a Charter Statement in the House of Commons on 2 December 2020. See Government of Canada, *Bill C-11: An Act to enact the Consumer Privacy Protection Act and the Personal Information and Data Protection Tribunal Act and to make related and consequential amendments to other Acts – Charter Statement*, 2 December 2020. This Legislative Summary incorporates much of the content of the Legislative Summary of Bill C-11 for the parts of the bill that are identical or similar. See also Sabrina Charland, Alexandra Savoie and Ryan van den Berg, *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*, Publication no. 43-2-C11-E, 10 December 2020.

3. For a more comprehensive history of the *Personal Information Protection and Electronic Documents Act* (PIPEDA) and of the calls for reform made 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.

4. Innovation, Science and Economic Development Canada (ISED), *Canada's Digital Charter: Trust in a digital world*. Canada's Digital Charter illustrates the government's plan to establish the trust that is the foundation of the digital and data-driven economy. It is not a legally binding legislative instrument; rather, it is a set of principles that the government will take into account when developing future policies, programs and legislation on the digital economy.

5. ISED, *Canada's Digital Charter in Action: A Plan by Canadians, for Canadians*.

6. ISED, *Strengthening Privacy for the Digital Age*.

7. Office of the Privacy Commissioner of Canada (OPC), *Privacy Law Reform: A Pathway to Respecting Rights and Restoring Trust in Government and the Digital Economy – 2018–2019 Annual Report*, 2019. Privacy by design is a concept that refers to considering privacy from the initial design of a product or service through to its deployment and long-term implementation, for example, using a privacy impact assessment.

8. OPC, *Privacy in a pandemic: 2019–2020 Annual Report to Parliament on the* Privacy Act *and* Personal Information Protection and Electronic Documents Act, 2020.

9. 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.

10. OPC, *Projecting our values into laws: Laying the foundation for responsible innovation – 2020–2021 Annual Report to Parliament on the* Privacy Act *and the* Personal Information Protection and Electronic Documents Act, 2021. Daniel Therrien's term as Privacy Commissioner ended on 3 June 2022. On 23 June 2022, Philippe Dufresne was appointed Privacy Commissioner for a seven-year term.

11. 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.

12. 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.

13. ETHI, *Collection and Use of Mobility Data by the Government of Canada and Related Issues*, Fourth report, May 2022.

14. OPC, *Submission of the Office of the Privacy Commissioner of Canada on Bill C-11, the* Digital Charter Implementation Act, *2020*, May 2021.

15. European Union (EU), 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) (Text with EEA relevance)*, Official Journal no. L 119, art. 45.

16. EU, 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*, Official Journal no. L 281; and Government of Canada, *The European Union's General Data Protection Regulation*.

17. EU, 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) (Text with EEA relevance)*, Official Journal no. L 119, art. 45, para. 9.

18. EU, European Commission, *Adequacy decisions*.

19. Government of Canada, *Sixth Update Report on Developments in Data Protection Law in Canada*, Report to the European Commission, December 2019.

20. EU, 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) (Text with EEA relevance)*, Official Journal no. L 119, art. 45, para. 3.

21. EU, EUR-Lex, *Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative acts*; and EU, European Parliament, *Artificial Intelligence Act*, Legislative Observatory, Database, accessed July 2022.

22. Clause 2 of the bill contains the full text of the Consumer Privacy Protection Act (CPPA) but does not include the preamble.

23. OPC, *Submission of the Office of the Privacy Commissioner of Canada on Bill C-11, the* Digital Charter Implementation Act, 2020, May 2021. The brief includes a proposed preamble, the first recital paragraph of which reads: "WHEREAS privacy is a basic human right of every individual and a fundamental value reflected in international human rights instruments to which Canada is a signatory." The OPC had previously recommended adding a preamble to the CPPA in its 2018–2019 annual report.

24. 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.

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

26. OPC, *Submission of the Office of the Privacy Commissioner of Canada on Bill C-11, the* Digital Charter Implementation Act, *2020*, May 2021.

27. OPC, *PIPEDA in brief*.

28. At this time, British Columbia, Alberta and Quebec have enacted legislation that is substantially similar to PIPEDA. In those provinces, PIPEDA is not applicable, except as concerns the commercial activities of federally regulated 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." In English, the term "substantially similar" is used in both.

29. 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 be applicable to the CPPA. See *A.T. v. Globe24h.com*, 2017 FC 114 (CanLII), para. 50.

30. The provisions on the accountability of organizations in sections 7 to 11 of the CPPA reflect the content of Principle 1 set out in Schedule 1 of PIPEDA.

31. Sections 12 to 14 of the CPPA reflect the content of Principle 2, Principle 4 and Principle 5 set out in Schedule 1 of PIPEDA. Section 15(7) of the CPPA also states that an organization "must not, as a condition of the provision of a product or service, require an individual to consent to the collection, use or disclosure of their personal information beyond what is necessary to provide the product or service."

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

33. Section 2 of the CPPA provides the following definition of dispose: "to permanently and irreversibly delete personal information or to anonymize it."

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

35. Section 62 of the CPPA reflects the content of Principle 8 set out in Schedule 1 of PIPEDA concerning openness.

36. Sections 63 to 71 of the CPPA reflect the content of Principle 9 set out in Schedule 1 of PIPEDA concerning access to personal information.

37. Sections 82 to 87 of the CPPA reflect the content of Principle 10 set out in Schedule 1 of PIPEDA.

38. Sections 9(1), 11(1), 12(3), 12(4), 13, 14(1), 15(1), 15(7), 16, 17(2), 53, 55(1), 55(4), 57(1), 58(1), 58(3), 61 and 62(1) of the CPPA.

39. Costs are expenses that the successful party can be paid by the other party. See, for example, Government of Canada, "Frais de justice : dépens et autres frais," *Guide fédéral de jurilinguistique législative française* [AVAILABLE IN FRENCH ONLY].

40. Section 2 of the Artificial Intelligence and Data Act (AI Act) provides that a "person" includes a trust, a joint venture, a partnership, an unincorporated association and any other legal entity.

41. Section 26 of the AI Act lists the following persons or entities: the Privacy Commissioner; the Canadian Human Rights Commission; the Commissioner of Competition; the Canadian Radio-television and Telecommunications Commission; any person appointed by the government of a province, or any provincial entity, with powers, duties and functions that are similar to those of the Privacy Commissioner or the Canadian Human Rights Commission; and any other person or entity prescribed by regulation.

42. Section 30(3) of the AI Act.

43. Section 38 of the AI Act refers to section 4(3) of the *Criminal Code* to define the term "possess." Section 4(3) provides that a person is in possession of an item when the person has it in their personal possession or knowingly "has it in the actual possession or custody of another person" or "has it in any place, whether or not that place belongs to or is occupied by him, for the use or benefit of himself or of another person." See *Criminal Code*, R.S.C. 1985, c. C-46, s. 4(3)(a).

44. Section 40 of the AI Act.