LIBRARY OF PARLIAMENT
BIBLIOTHÈQUE DU PARLEMENT

PRELIMINARY VERSION

UNEDITED

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

Legislative Summary

BILL C-36:
AN ACT TO ENACT THE PROTECTING PRIVACY AND CONSUMER DATA ACT, TO AMEND THE PERSONAL INFORMATION PROTECTION AND ELECTRONIC DOCUMENTS ACT AND TO MAKE AMENDMENTS TO OTHER ACTS

45-1-C36-E

6 July 2026

Alexandra Savoie and Maxime-Olivier Thibodeau

Library and Research Services

PRELIMINARY VERSION
UNEDITED

AUTHORSHIP

6 July 2026 Alexandra Savoie and Maxime-Olivier Thibodeau

ABOUT THIS PUBLICATION

Library of Parliament legislative summaries summarize bills currently before Parliament and provide background information about them in an objective and impartial manner. They are prepared by Library and Research Services, which carries out research for and provides information and analysis to parliamentarians, 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 Senate and House of Commons 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 to this Library of Parliament legislative summary that have been made since the preceding issue are indicated in **bold print**.

© Library of Parliament, Ottawa, Canada, 2026

Legislative Summary of Bill C-36
(Preliminary version)

45-1-C36-E

Ce document est également publié en français.

PRELIMINARY VERSION
UNEDITED

CONTENTS

1 BACKGROUND 1

1.1 History of the Bill 2

1.2 New Artificial Intelligence Strategy 3

1.3 Adequacy Status with the European Union 3

2 DESCRIPTION AND ANALYSIS 4

2.1 Protecting Privacy and Consumer Data Act (Clause 1 of Bill C-36, Sections 1 to 75 of the PPCDA) 4

2.1.1 Authorized Representatives (Section 4 of the PPCDA) 5

2.1.2 Purpose (Section 5 of the PPCDA) 6

2.1.3 Application (Section 6 of the PPCDA) 6

2.1.4 Accountability of Organizations (Sections 7 to 11 of the PPCDA) 7

2.1.5 Appropriate Purposes for the Collection, Use and Disclosure of Personal Information, and Applicable Limitations (Sections 12 to 14 of the PPCDA) 8

2.1.6 Consent (Sections 15 to 17 of the PPCDA) 9

2.1.7 Exceptions to the Requirement for Consent (Sections 18 to 50 of the PPCDA) 10

2.1.8 Retention, Disposal and Accuracy of Personal Information (Sections 52 to 55 of the PPCDA) 12

2.1.9 Security Safeguards (Sections 56 to 60 of the PPCDA) 14

2.1.10 Openness and Transparency (Section 62 of the PPCDA) 14

2.1.11 Access to and Amendment of Personal Information (Sections 63 to 71 of the PPCDA) 16

2.1.12 Mobility of Personal Information (Section 72 of the PPCDA) 17

2.1.13 De-identification of Personal Information (Sections 74 and 75 of the PPCDA) 18

2.2 Digital Safety and Data Protection Commission of Canada (Clauses 8 to 25 of Bill C-36) 18

2.2.1 Long and Alternative Titles of the Act Establishing the Digital Safety Commission (Clauses 8 and 9 of Bill C-36) 18

PRELIMINARY VERSION
UNEDITED

2.2.2 Definition and Establishment of the Digital Safety and Data Protection Commission of Canada (Clauses 10 and 11 of Bill C-36) 19
2.2.3 New Section 6(1.1) of the Digital Safety and Data Protection Commission of Canada Act (Clause 12 of Bill C-36) 19
2.2.4 Composition of the Digital Safety and Data Protection Commission of Canada (Clause 13 of Bill C-36) 19
2.2.5 Contracts, Memoranda of Understanding, or Other Agreements or Arrangements Entered into by the Digital Safety and Data Protection Commission of Canada (Clause 14 of Bill C-36) 19
2.2.6 Exclusion of Personal Information from the Digital Safety and Data Protection Commission of Canada's Annual Report (Clause 15 of Bill C-36) 20
2.2.7 Definitions (Clause 16 of Bill C-36) 20
2.2.8 Factors to be Taken into Account when Making Regulations and Issuing Guidelines, Codes of Conduct and Other Documents for the Purposes of the Digital Safety Act (Clause 17 of Bill C-36) 20
2.2.9 Repeal of Section 122 of the Digital Safety Act (Clause 18 of Bill C-36) 20

2.3 Protecting Privacy and Consumer Data Act (Clause 1 of Bill C-36, Sections 76 to 147 of the PPCDA) 21
2.3.1 The Digital Safety and Data Protection Commission of Canada (Sections 76 to 84 of the PPCDA) 21
2.3.2 The Privacy and Consumer Data Commissioner (Sections 85 to 88 of the PPCDA) 25
2.3.3 The Privacy and Consumer Data Division (Sections 89 to 91 of the PPCDA) 25
2.3.4 Codes of Practice and Certification Programs (Sections 92 to 96 of the PPCDA) 26
2.3.5 Remedies (Sections 97 to 120 of the PPCDA) 27
2.3.6 Powers of the Commission and Commissioner: Investigations, Audits and Proceedings (Sections 121 to 125 of the PPCDA) 33
2.3.7 Appeals (Sections 126 to 128 of the PPCDA) 34
2.3.8 Enforcement of Orders (Sections 129 to 131 of the PPCDA) 35
2.3.9 Private Right of Action (Section 132 of the PPCDA) 36
2.3.10 Certificate Under the *Canada Evidence Act* (Sections 133 to 138 of the PPCDA) 36
2.3.11 General (Sections 139 to 146 of the PPCDA) 38
2.3.12 Coming into Force (Section 147 of the PPCDA) 40

PRELIMINARY VERSION
UNEDITED

2.4 Amendment to the *Personal Information Protection and Electronic Documents Act* (Clauses 2 to 7 of Bill C-36) 40

2.5 Consequential and Related Amendments, Transitional Provision, Coordinating Amendments and Coming into Force (Clauses 26 to 52 of Bill C-36) 41

PRELIMINARY VERSION
UNEDITED

LEGISLATIVE SUMMARY OF BILL C-36: AN ACT TO ENACT THE PROTECTING PRIVACY AND CONSUMER DATA ACT, TO AMEND THE PERSONAL INFORMATION PROTECTION AND ELECTRONIC DOCUMENTS ACT AND TO MAKE AMENDMENTS TO OTHER ACTS

1 BACKGROUND

On 15 June 2026, the Minister of Artificial Intelligence and Digital Innovation introduced in the House of Commons Bill C-36, An Act to enact the Protecting Privacy and Consumer Data Act, to amend the Personal Information Protection and Electronic Documents Act and to make amendments to other Acts (Bill C-36).[1]

The bill creates a new law, the Protecting Privacy and Consumer Data Act (PPCDA). It repeals Part 1 of the *Personal Information Protection and Electronic Documents Act* (PIPEDA) and changes the short title of that Act to the *Electronic Documents Act*.[2]

In general, the PPCDA:

- codifies the contents of the fair information principles set out in Schedule 1 of PIPEDA by rewording them as legislative provisions;
- amends the definition of personal information to include information that is inferred about an identifiable individual and adds a definition of what constitutes sensitive personal information, which includes a child's personal information (section 2);
- explicitly recognizes the fundamental right of privacy of individuals (section 5);
- 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 a new exception regarding an organization's business activities (section 18);
- includes the right to erasure (section 54);
- requires organizations to carry out a privacy impact assessment before any personal information is disclosed or transferred outside Canada (section 57);
- 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);

PRELIMINARY VERSION
UNEDITED

- 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);
- gives a new Digital Safety and Data Protection Commission of Canada (the Commission), rather than the Privacy Commissioner of Canada, the responsibility for ensuring compliance with the PPCDA, (art. 76);
- recognizes the principle of the best interests of children as a factor that the Commission must take into account in exercising any powers or performing any duties under the PPCDA (sections 77, 86 and 90);
- grants the Commission the ability to impose a maximum penalty that is the higher of $10 million or 3% of an organization's gross global revenue from the previous year for contravening certain specific provisions of the PPCDA (sections 113 and 114); and
- provides for a maximum fine not exceeding the higher of $25 million or 5% of an organization's gross global revenue from the previous year in the case of a conviction for contravening certain specific provisions of the PPCDA or in the case of obstructing the Commission's work (section 145).

The Commission is established by Bill C-34, An Act to enact the Digital Safety Act and the Digital Safety Commission of Canada Act and to make consequential amendments to other Acts, which was introduced in the House of Commons by the Minister of Canadian Identity and Culture and Minister responsible for Official Languages on 10 June 2026 (Bill C-34).[3] Unlike the current Privacy Commissioner of Canada, the Commission ultimately reports to a minister rather than to Parliament. The Commission will be established once Bill C-34 is passed.

1.1 HISTORY OF THE BILL

There have been many calls to reform PIPEDA over the past 10 years, particularly by the Privacy Commissioner of Canada and by the House of Commons Standing Committee on Access to Information, Privacy and Ethics.[4] Bill C-36 is the latest attempt to modernize the legislation, following two previous attempts between 2020 and 2025.

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, was introduced in the House of Commons on 17 November 2020 (Bill C-11).[5] It was the first bill seeking to fully reform PIPEDA since it was passed in 2000.[6] It died on the *Order Paper* when Parliament was dissolved in August 2021.

PRELIMINARY VERSION
UNEDITED

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, was introduced in the House of Commons on 16 June 2022 (Bill C-27).[7]

Bill C-27 replicated the contents of Bill C-11, but it also sought to establish a regulatory framework for artificial intelligence (AI) at the federal level.[8] It passed second reading and was referred to committee on 24 April 2023. Following an extensive study of the bill, the committee began clause-by-clause consideration but did not complete it.[9] The bill died on the *Order Paper* when Parliament was dissolved in January 2025.

Bill C-36 incorporates much of the content in Bill C-27, but it does not contain a preamble, nor does it propose creating a Personal Information and Data Protection Tribunal or enacting an Artificial Intelligence and Data Act.

1.2 NEW ARTIFICIAL INTELLIGENCE STRATEGY

On 4 June 2026, the Government of Canada unveiled Canada's National Artificial Intelligence Strategy: AI for All.[10] This strategy recognizes that AI raises several important questions, including questions related to privacy protection. Its first pillar, "Protecting Canadians and safeguarding our democracy," states the following:

> AI will only deliver on its promise if Canadians trust it. That requires modern privacy and online safety laws, strong national AI safety capabilities, and secure government systems.[11]

The strategy indicates that Canada will modernize consumer privacy legislation to enshrine a fundamental right to privacy, safeguard children's information from exploitation and harm, and strengthen people's control over their personal data. It also indicates that Canada will strengthen its privacy laws to ensure that Canadians' personal information is not used inappropriately, including for surveillance pricing.[12]

Bill C-36 is one of the vehicles chosen by the government to meet these objectives.[13]

1.3 ADEQUACY STATUS WITH THE EUROPEAN UNION

Any attempt to modernize PIPEDA must consider maintaining Canada's adequacy status with the European Union (EU). In 2001, under Directive 95/46/EC in effect at that time, the European Commission (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.[14]

PRELIMINARY VERSION
UNEDITED

The EU's General Data Protection Regulation (GDPR), which entered into force on 25 May 2018, replaced the above-mentioned directive. It provided for the continuity of existing EU adequacy decisions until a new assessment could be conducted.[15] In 2024, the EC reaffirmed Canada's adequacy status, even though PIPEDA had not undergone any significant reform.[16]

Maintaining Canada's adequacy status has the advantage of ensuring 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).[17]

The EU will soon be reassessing the adequacy of Canada's federal private-sector privacy laws as they compare to the GDPR. A reassessment must be conducted at least every four years, which means that the next one should take place no later than 2028.[18]

Replacing PIPEDA with a new law and changing the organization responsible for enforcing it could have an impact on this assessment.

2 DESCRIPTION AND ANALYSIS

Bill C-36 contains 52 clauses and is divided into four parts:

- Part 1 contains the full text of the new PPCDA.
- Part 2 contains amendments to Part 2 of PIPEDA, which becomes the Electronic Documents Act.
- Part 3 contains amendments to the Digital Safety Act and the Digital Safety Commission of Canada Act (proposed in Bill C-34), including amendments to change the name of the Commission and to refer to that Commission and the PPCDA in the relevant provisions of those Acts.
- Part 4 contains the consequential and related amendments, the transitional provision, the coordinating amendments and the coming into force provision.

The description and analysis that follow focus on key aspects of the bill. Only the main provisions are examined.

2.1 PROTECTING PRIVACY AND CONSUMER DATA ACT (CLAUSE 1 OF BILL C-36, SECTIONS 1 TO 75 OF THE PPCDA)

Clause 1 of the bill includes the full text of the PPCDA, which is presented as an Act "to support and promote digital commerce by protecting personal information that is collected, used or disclosed in the course of commercial activities."

PRELIMINARY VERSION
UNEDITED

The PPCDA is divided into three parts. Part 1 addresses the obligations of organizations as they relate to the protection of personal information (sections 7 to 75). Part 2 mainly deals with the powers, duties and functions of the Commission and of the member of that Commission who is designated as the Privacy and Consumer Data Commissioner. It also contains general provisions (sections 76 to 146). Part 3 addresses the coming into force of its provisions (section 147).[19]

Like the proposed Consumer Privacy Protection Act (CPPA) in Bill C-27, the PPCDA 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.[20] In the PPCDA, these principles are incorporated into the text of the Act, using conventional legislative wording.

The PPCDA reintroduces much of what was in the CPPA (Bill C-27), which Bill C-27 proposed to enact, with some amendments, additions and deletions. The significant differences between the provisions of the PPCDA and the corresponding provisions of the CPPA (Bill C-27) are identified in the relevant sections of this legislative summary.

2.1.1 Authorized Representatives (Section 4 of the PPCDA)

Under section 4 of the PPCDA, the rights provided for under the PPCDA, including any right of recourse, may be exercised on behalf of a child, by a parent, guardian or tutor, unless the child wishes to personally exercise those rights and is capable of doing so; on behalf of an individual, other than a child, under a legal incapacity, by a person authorized by law to administer the affairs or property of that individual; on behalf of a deceased individual, by a person authorized by law to administer the estate or succession of that individual, but only for the purpose of that administration; and on behalf of any other individual, by a person authorized in writing by that individual to do so.

The fourth type of authorized representative identified was not included in the corresponding provision of the CPPA (Bill C-27). The PPCDA also indicates that the authorized representative who administers the estate or succession of a deceased individual can do so only for the purposes of that administration.

For the purposes of this section, the term “child” is defined as an individual who is under 18 years of age. Bill C-27 used the term “minor” rather than child.

PIPEDA does not contain any provisions regarding authorized representatives.

PRELIMINARY VERSION
UNEDITED

2.1.2 Purpose
(Section 5 of the PPCDA)

The purpose of the PPCDA 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).

However, the PPCDA does make two important changes. First, as was the case with the CPPA (Bill C-27), these rules are being established in a different context. They are now being 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).[21] Second, the purpose of the PPCDA recognizes the right of privacy of individuals is a fundamental right, something that was not recognized in the purpose of the CPPA (Bill C-27). The Privacy Commissioner of Canada recommended that this recognition be added.[22]

2.1.3 Application
(Section 6 of the PPCDA)

The application of the PPCDA is the same as that of PIPEDA. The PPCDA 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 applies to the personal information of employees of federally regulated private businesses (e.g., banks and telecommunications companies).[23]

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

The PPCDA 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 PPCDA under section 139(2)(b), within a province (section 6(2)). Furthermore, section 139(2)(b) sets out the process by which a province may have its provincial legislation recognized as "substantially similar" to the PPCDA.[24]

The PPCDA also states that it does not apply in respect of personal information that has been anonymized (section 6(5)).

PRELIMINARY VERSION
UNEDITED

The term "anonymize" is defined as follows in section 2 of the PPCDA:

> [T]o irreversibly and permanently modify personal information to ensure that there is no reasonably foreseeable risk in the circumstances that an individual can be identified from the information, whether directly or indirectly, by any means.[25]

This definition differs slightly from that set out in the CPPA (Bill C-27).

The PPCDA also makes a distinction between anonymized information and de-identified personal information.

The term "de-identify" is defined as follows in section 2 of the PPCDA: "to modify personal information so that an individual cannot be directly identified from it, although a risk of the individual being identified remains." This definition differs slightly from the definition of the same term set out in the CPPA (Bill C-27).

The PPCDA does not contain any explicit provisions concerning its extraterritorial application to organizations that do not operate in Canada.[26]

2.1.4 Accountability of Organizations (Sections 7 to 11 of the PPCDA)

Under the PPCDA, all organizations are accountable for personal information under their control.[27] Information is under the control of an organization when it determines the purposes for its collection, use or disclosure. The PPCDA states that an organization retains this accountability, even if a service provider carries out the activities on its behalf (section 7).

The obligations set out in the PPCDA do not apply to a service provider in terms of the information transferred to it by an organization, except for those relating to breach of security safeguards. They do apply, however, if the service provider collects, uses or discloses the personal information for purposes other than those for which the information was transferred to it. The organization must ensure that all service providers to which it transfers personal information provide the same protection that it provides under the PPCDA, itself (sections 7 and 11).

Every organization must designate at least one individual to be responsible for matters related to its obligations under the PPCDA. Organizations must also implement and maintain a privacy management program (the program) that includes the policies, practices and procedures the organization has put in place to fulfill its obligations. The program takes into account the volume of personal information under the organization's control and the sensitivity of that information (sections 8 and 9).

Section 2 of the PPCDA defines "sensitive" personal information as personal information in respect of which, taking into account the circumstances, an individual has a heightened expectation of privacy (e.g., a child's personal information).[28] No such definition was included in the CPPA (Bill C-27).

The organization must give the Commission access to the program, on request. The Commission may, after reviewing the program, provide guidance or recommend that corrective measures be taken by the organization (section 10).

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

Sections 12 to 14 of the PPCDA apply a necessity and proportionality test for the collection, use and disclosure of personal information.[29]

The PPCDA states that an organization may 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 factors to take into account in determining whether the manner and purposes of collecting, using or disclosing personal information are appropriate:

- the sensitivity of the personal information;
- whether the purposes represent legitimate business needs of the organization;
- the degree of effectiveness of the collection, use or disclosure in meeting these needs;
- whether there are 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 in light of the measures, technical or otherwise, implemented by the organization to mitigate the impacts of the loss of privacy on the individual.

The organization must determine at or before the time of the collection of any personal information the purposes for which the information is or is to be collected, and those purposes must be recorded (section 12(3)). The PPCDA does not specify how those purposes are to be recorded. If an organization wants to use or disclose the information it has collected for a new purpose, it must first record that new purpose and obtain the individual's valid consent, unless an exception to the requirement for consent applies (sections 12(4), 13 and 14).

PRELIMINARY VERSION
UNEDITED

2.1.6 Consent
(Sections 15 to 17 of the PPCDA)

Consent remains the default legal basis for an organization to collect, use and disclose personal information under the PPCDA (section 15).

Under the PPCDA, consent is valid only if the organization provides the individual with certain prescribed information (section 15(3)):

- the purposes for the collection, use or disclosure of the personal information;
- the manner 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.

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 (section 15(4)).

In contrast, 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[30].

The criterion regarding an individual's understanding of the nature, purposes and consequences of the collection, use and disclosure of their personal information has been removed from the definition of valid consent in the PPCDA.

In addition to the above, under the PPCDA, an organization may determine that implied consent is appropriate in some circumstances, taking into account the sensitivity of the personal information and the reasonable expectations of the individual (section 15(5)).

An organization must not obtain or attempt to obtain an individual's consent by using deceptive or misleading practices (section 16). On giving reasonable notice to an organization, an individual may, at any time, subject to the PPCDA, to federal or provincial law or to the "reasonable" terms of a contract, withdraw their consent (section 17).

PRELIMINARY VERSION
UNEDITED

2.1.7 Exceptions to the Requirement for Consent (Sections 18 to 50 of the PPCDA)

Without consent, an organization must justify the collection, use or disclosure of personal information without the knowledge or consent of the concerned individual based on an exception. There are six categories of exceptions:

- the organization's business activities (sections 18 to 28);
- public interest (sections 29 to 37);
- investigations (sections 38 to 41);
- disclosures to government institutions (sections 42 to 47);
- required by law (sections 48 and 49); and
- publicly available information (section 50).

The exceptions set out in sections 23 to 50 essentially mirror the content of sections 7 and 7.2 to 7.4, and sections 10.2(3) and 10.2(4) of PIPEDA. Only the new exceptions set out in the PPCDA are examined below.

Section 18 of the PPCDA sets out a new exception to the consent requirement related to "business activities." This exception enables an organization to collect or use an individual's personal information without their knowledge or consent if the collection or use is made for the purposes of certain business activities (section 18(1)). The collection or use must meet two conditions:

- a reasonable person would expect the collection or use for such an 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 an activity that is necessary to provide a product or service that the individual has requested, an activity that is "necessary for the security of the organization's information, systems or networks" and an activity that is "necessary for the safety of a product or service that the organization provides," as well as any other prescribed activity (section 18(2)).

An organization may also collect, use or disclose an individual's personal information without their knowledge or consent if the collection, use or disclosure is made for the purpose of an activity in which the organization has a "legitimate interest that outweighs any reasonably foreseeable adverse effect on the individual that could result from that collection, use or disclosure" (section 18(3)) and if the two above-mentioned conditions set out in section 18(1) are met. In the corresponding provision of the CPPA (Bill C-27), the legitimate interest must outweigh "any potential adverse effect" rather

than "any reasonably foreseeable adverse effect." The scope of the exception therefore appears to be slightly broader under the PPCDA.

Other conditions precedent must also be met before an organization can make use of the "legitimate interest" exception. The organization must record the description of its "legitimate interest" in the proposed activity and carry out a privacy impact assessment (PIA) to identify any reasonably foreseeable adverse effect that is likely to result from the collection, use or disclosure of the personal information. The organization must also identify and take reasonable measures to reduce the likelihood that the adverse effects will occur or to mitigate or eliminate them, and the organization must comply with any prescribed requirements (sections 18(4) and 18(5)).

The CPPA (Bill C-27) did not require the organization to identify and describe its legitimate interest in the proposed activity or to carry out a PIA as conditions precedent. It also limited the application of the "legitimate interest" exception to the collection and use of personal information. Under the PPCDA, this exception can also be used to disclose an individual's personal information without their knowledge or consent.

Under the PPCDA, an organization may transfer an individual's personal information to a service provider without their knowledge or consent (section 19). It may use an individual's personal information without their knowledge or consent to de-identify or anonymize the information (section 20). An organization may also use an individual's personal information without their knowledge or consent for the organization's internal research, analysis and development purposes if the information is de-identified before it is used (section 21).

The PPCDA provides that an organization may use and disclose an individual's personal information without their knowledge or consent for the purposes of a prospective business transaction, but only if the information is de-identified (section 22). PIPEDA already sets out a similar exception, but it applies to personal information, not to personal information that has been de-identified.[31]

However, an organization is not required to comply with the requirement that all information be de-identified before being disclosed for the purposes of a prospective business transaction if doing so would undermine the objectives for carrying out the transaction and the organization has taken into account the risk of harm to the individual that could result from using or disclosing the personal information (section 22(2)). PIPEDA does not provide for such an exception.

The PPCDA provides for a new exception that allows an organization to disclose an individual's personal information without their knowledge or consent to another organization under section 11.01(1) of the *Proceeds of Crime (Money Laundering) and Terrorist Financing Act* (section 41).[32] This exception is in addition to the

exception to the consent requirement related to section 7 of this Act that is already set out in PIPEDA.[33]

Furthermore, the CPPA (Bill C-27) set out an exception about sharing personal information for a socially beneficial purpose.[34] This exception is not included in the PPCDA. The same is true of the exception regarding statistics, study or research that is set out in PIPEDA and that was also included in the CPPA (Bill C-27).[35]

2.1.8 Retention, Disposal and Accuracy of Personal Information (Sections 52 to 55 of the PPCDA)

Sections 52 to 55 of the PPCDA deal with the retention period for personal information, the right to request its disposal and the accuracy of that information.

An organization must take into account the sensitivity of the personal information when determining the retention period. An organization must not retain personal information for a period longer than necessary to fulfill the purposes for which the information was collected, used or disclosed, or to comply with the requirements of the PPCDA, of federal or provincial law, or of the reasonable terms of a contract (section 52). An organization that uses personal information to make a decision about an individual must retain that information for a sufficient period of time to permit the individual to make a request for access (section 53).

An organization must also take reasonable steps to ensure that personal information under its control is accurate, up to date and complete, unless the information has been de-identified. In determining whether the information must be updated, the organization must take into account the individual's interests, including whether the information may be used to make a decision about the individual, whether the information is used on an ongoing basis and whether the information is disclosed to third parties (section 55).[36] The exception for de-identified information was not included in the corresponding provision of the CPPA (Bill C-27).

The PPCDA also includes an explicit right to request the disposal of personal information that was not found in PIPEDA (section 54). This is a form of right to erasure. If an organization receives a written request from an individual to dispose of their personal information that is under the organization's control, the organization must do so, as soon as feasible, under three circumstances: the information was collected, used or disclosed in contravention of the PPCDA; the individual has withdrawn their consent; or the information is no longer necessary (section 54(1)).

Section 2 of the PPCDA defines the term "dispose" as follows: "to permanently and irreversibly delete personal information or to anonymize it."

PRELIMINARY VERSION
UNEDITED

An organization may refuse a request to dispose of personal information in one or more of the following circumstances:

- the disposal of the information would result in the disposal of personal information about another individual and the information cannot be severed without imposing an undue burden on the organization;
- there are other requirements of a relevant law or of the reasonable terms of a contract that prevent the organization from disposing of the information;
- the information is necessary for the establishment of a legal defence or in the exercise of other legal remedies by the organization;
- the information is not in relation to a child and the disposal of the information would have an undue adverse effect 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 disposal of the information would have an undue adverse effect on the organization that outweighs any potential adverse effect on the individual resulting from the retention of the information.

The conditions for refusing to dispose of personal information are similar to those that were set out in the corresponding provision of the CPPA (Bill C-27).[37] However, the first condition is now limited to cases where it is impossible to sever the personal information "without imposing an undue burden on the organization." The concept of an "undue burden" is new.

The final condition for refusing to dispose of personal information, which has to do with an undue adverse effect on the organization, is also new. It replaces the final condition of the corresponding provision of the CPPA (Bill C-27), which enabled an organization to refuse a request to dispose of personal information if the information was not in relation to a minor, it was scheduled to be disposed of in accordance with the organization's information retention policy and the organization informed the individual of the remaining period of time for which the information would be retained.[38] The Privacy Commissioner of Canada recommended removing this condition.[39]

When an organization refuses to dispose of an individual's personal information, it must inform the individual in writing of the refusal, setting out the reasons. The organization must also inform the individual that they have the right to make a complaint to the organization or to the member of the Commission who is designated as the Privacy and Consumer Data Commissioner. In the case of a request that is refused because it would have an undue adverse effect on the organization, the organization must inform the Commission of the refusal (section 54(4)).

The organization must also inform any service provider to which it has transferred the information of the request for disposal, and if so, ensure that the service provider disposes of the information (section 54(5)).

2.1.9 Security Safeguards (Sections 56 to 60 of the PPCDA)

Under the PPCDA, an organization must protect the personal information that it holds.[40] It must do so through physical, organizational and technological security safeguards. The level of protection provided by those safeguards must be proportionate to the sensitivity of the personal information. The safeguards must also take into account the quantity, distribution, format and method of storage of the information, as well as any reasonably foreseeable privacy implications that may arise in relation to the transfer of personal information to a service provider (section 56). The corresponding provision of the CPPA (Bill C-27) did not make any reference to the potential implications of the transfer of personal information to a service provider.

An obligation regarding the disclosure or transfer of personal information outside Canada is also found in the PPCDA. An organization must carry out a PIA and implement measures to mitigate the risks before disclosing or transferring the information. Such measures can include contractual measures or adherence to a code of practice or an approved certification process. On request, an organization must provide the Commission with a copy of the PIA (section 57). No such obligation was found in the CPPA (Bill C-27).

The PPCDA also establishes a system for reporting breaches of security safeguards. Like the CPPA (Bill C-27), it essentially reiterates the content of sections 10.1 to 10.3 of PIPEDA, except with regard to the entity to which a breach must be reported (sections 58 to 60). Any breach must be reported to the Commission rather than to the Privacy Commissioner of Canada.

Like the CPPA (Bill C-27), the PPCDA indicates that if a service provider determines that any breach of security safeguards has occurred that involves personal information, it must, as soon as feasible, notify the organization that controls the personal information (section 61). That point is not included in PIPEDA.

2.1.10 Openness and Transparency (Section 62 of the PPCDA)

Under the PPCDA, an organization must make readily available information that explains the organization's policies and practices put in place to fulfill its obligations under this Act.[41] This information must be provided in plain language. It includes:

- a description of the type of personal information under the organization's control;

PRELIMINARY VERSION
UNEDITED

- 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;
- a general account of the organization's use of any automated decision system to make predictions, recommendations or decisions that could have a legal or similarly significant effect on individuals;
- whether or not the organization transfers or discloses personal information interprovincially or outside of Canada that may have reasonably foreseeable privacy implications;
- the retention periods applicable to sensitive personal information;
- how an individual may make a request for disposal or access; and
- the business contact information of the individual to whom complaints or requests for information may be made.

An organization is required to make available information about cross-border data transfers it carries out only if it has determined that these exchanges may have reasonably foreseeable privacy implications.

Section 62 of the PPCDA includes the concept of algorithmic transparency in the form of a right to explanation. This right to explanation is fleshed out further in section 63. Section 2 of the PPCDA defines the term "automated decision system" as follows:

> [A]ny 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[42].

An organization is required to provide a general account of its use of any automated decision system to make predictions, recommendations or decisions about individuals only when doing so could have a "legal" or "significant effect" on them.

In its submission on Bill C-27, the Privacy Commissioner of Canada recommended eliminating the "significant effect" criterion from the corresponding provision of the CPPA (Bill C-27), noting the following:

> Limiting the general account requirement to activities with a "significant impact" would likely strike a reasonable balance between providing transparency for individuals and compliance effort for organizations. However, its addition to the explanation requirement is a problematic change from the former Bill C-11, as it narrows the scope of the requirement and would likely exclude decisions for matters

> such as online advertising, personalized news feeds and digital environments. As a result, narrowing this requirement to only those with significant impacts would not be in the interest of achieving algorithmic transparency.[43]

The corresponding provision of the CPPA (Bill C-27) did not include the concept of "legal effect." Otherwise, it was essentially the same as the provision in the PPCDA.

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

On request by an individual, an organization must inform them of whether it has any personal information about them, and if so, how it uses the information and whether it has disclosed the information to third parties. It must also give the individual access to the information. However, the organization is not required to act on a request in respect of de-identified personal information (section 63). The exception regarding de-identified personal information was not included in the corresponding provision of the CPPA (Bill C-27).

If the organization has used an automated decision system to make a prediction, recommendation or decision about the individual that could have a legal or similarly significant effect on them, the organization must, on request by the individual, provide them with an explanation of the prediction, recommendation or decision. The explanation must indicate the type of personal information that was used, the source of the information and the reasons or principal factors that led to the prediction, recommendation or decision. The organization must also provide an individual with an opportunity to make written representations to an employee of the organization who is able to review the prediction, recommendation or decision. The PPCDA therefore includes a form of human oversight over automated decision systems (sections 63(4) to 63(6) and 66(1)). No such oversight was provided for in the CPPA (Bill C-27).

The PPCDA requires the organization to provide all the information requested under section 63 to the individual in plain language (section 66), which should prevent the communication of lengthy documents written in complex legal terms.[44]

The organization must respond to the information request no later than 30 days after the day on which it is received unless the organization extends the time limit for one of the prescribed reasons. The organization must send a notice of extension to the individual advising them of the reasons for extending the time limit and their right to make a complaint to the Commissioner. Any refusal to respond to a request must be justified; in this case, the organization must set out to the individual the reasons for refusal and any recourse that they may have (section 67).

PRELIMINARY VERSION
UNEDITED

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 must be retained long enough to allow the individual to exhaust any recourse they may have under the PPCDA (section 69).

In some cases, organizations may be prohibited from disclosing personal information. For example, an organization must not give an individual access to personal information if doing so would reveal personal information about another individual, unless : the information about the other individual is severable from the information about the requester without imposing an undue burden on the organization; the other individual consents to the access; or the requester needs the information because an individual's life, health or security is threatened (sections 70(1) and 70(2)).

Other circumstances may justify a refusal to disclose information, for example, when the request concerns communications between an organization and a government institution, and the institution, which must be consulted, objects to the disclosure of personal information for a valid reason such as a risk to national security (sections 70(3) to 70(6)).

The organization is not required to give the requester access to personal information in certain other cases. For example, if the information in question is protected by solicitor–client privilege or the professional secrecy of notaries, or to do so would reveal confidential commercial information that is impossible to sever without imposing an undue burden on the organization (section 70(7)).

With regard to the severing of personal information, as in section 54, the concept of an "undue burden" on the organization set out in section 70 is new. It was not included in the corresponding provision of the CPPA (Bill C-27).

If an individual has been given access to their personal information and demonstrates that the information is not accurate, up to date or complete, the organization must amend the information as required and transmit the amended information to any third party that has access to the information. This obligation does not apply in the case of de-identified personal information (section 71). This exception was not included in the corresponding provision of the CPPA (Bill C-27).

2.1.12 Mobility of Personal Information (Section 72 of the PPCDA)

The PPCDA 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 PPCDA, this transfer is

allowed only if both organizations involved are subject to a data mobility framework. The organization is not required to disclose de-identified personal information (section 72). This exception was not included in the corresponding provision of the CPPA (Bill C-27).

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

The PPCDA 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." It indicates that the organization must consider the risk of an individual being identified when applying technical and administrative measures to the information (section 74). This was not included in the corresponding provision of the CPPA (Bill C-27).

The PPCDA also prohibits an organization from using de-identified personal information, alone or in combination with other information, to identify an individual except in certain cases. These cases include the conduct of testing of the effectiveness of security safeguards that it has put in place, the conduct of testing of the effectiveness of its de-identification processes; and the conduct of testing of the effectiveness of the fairness and accuracy of models, processes and systems that were developed using de-identified personal information (section 75). The number of cases in which an organization may use de-identified personal information to identify an individual is higher in the PPCDA than under the corresponding provision of the CPPA (Bill C-27). Sections 75(b) to 75(e) of the PPCDA are new. They provide for the possibility that an organization may use de-identified personal information for the purpose of anonymizing it under section 20 or to comply with any requirements under the PPCDA or under federal or provincial law.

2.2 DIGITAL SAFETY AND DATA PROTECTION COMMISSION OF CANADA (CLAUSES 8 TO 25 OF BILL C-36)

2.2.1 Long and Alternative Titles of the Act Establishing the Digital Safety Commission (Clauses 8 and 9 of Bill C-36)

Clauses 8 and 9 of Bill C-36 amend the long and alternative titles of the Digital Safety Commission of Canada Act (Commission Act) set out in clause 4 of Bill C-34 and section 1 of the proposed Commission Act. They add the words "and Data Protection" after "Digital Safety" and before "Commission of Canada" in order to reflect the changes made by Bill C-36—which concerns data protection—to the provisions of Bill C-34, which deals with digital safety.

PRELIMINARY VERSION
UNEDITED

Although these two bills were introduced a few days apart, they must be considered together since one amends the other and the Commission is responsible for enforcing both the Digital Safety Act, enacted by Bill C-34, and the PPCDA, enacted by Bill C-36.

2.2.2 Definition and Establishment of the Digital Safety and Data Protection Commission of Canada (Clauses 10 and 11 of Bill C-36)

Clause 10 amends the definition of "Commission" set out in section 2 of the Commission Act by adding the words "and Data Protection" after "Digital Safety" and before "Commission of Canada." Clause 11 makes the same change to section 4 of the Commission Act, which provides for the establishment of the Commission.

2.2.3 New Section 6(1.1) of the Digital Safety and Data Protection Commission of Canada Act (Clause 12 of Bill C-36)

Clause 12 adds a new section 6(1.1) to the Commission Act, which provides that the Commission exercises the powers and perform the duties and functions conferred on it under the PPCDA. Section 6(1) provides that the Commission exercises the powers and performs the duties and functions conferred on it under the Digital Safety Act.

2.2.4 Composition of the Digital Safety and Data Protection Commission of Canada (Clause 13 of Bill C-36)

Clause 13 amends section 10 of the Commission Act so that the Commission consists of five full-time members – rather than three to five as provided for under Bill C-34 – to be appointed by the Governor in Council to hold office during good behaviour. The Governor in Council may remove a member at any time for cause.

2.2.5 Contracts, Memoranda of Understanding, or Other Agreements or Arrangements Entered into by the Digital Safety and Data Protection Commission of Canada (Clause 14 of Bill C-36)

Clause 14 amends section 19 of the Commission Act to state that the Chairperson of the Commission may enter into contracts, memoranda of understanding or other agreements or arrangements either in the name of His Majesty or in the name of the Commission except agreements or arrangements referred to in section 120 of the Digital Safety Act, but also in section 79, 80(1), 81(2), 82(3) and 82(4) of the PPCDA (see section 2.3.1 of this legislative summary).

PRELIMINARY VERSION
UNEDITED

2.2.6 Exclusion of Personal Information from the Digital Safety and Data Protection Commission of Canada's Annual Report (Clause 15 of Bill C-36)

Clause 15 amends section 22 of the Commission Act to specify that the Commission's annual report to the minister (under section 21(1) of that Act) must not contain "personal information," as defined in section 2(1) of the PPCDA. That section defines personal information as "information about an identifiable individual, including information that is inferred about the individual." Prior to amendment, this provision states that the report in question must not contain "personal information" as defined in section 3 of the *Privacy Act*.

2.2.7 Definitions (Clause 16 of Bill C-36)

Clause 16 amends the definitions of "Commission" and "personal information" set out in section 2(1) of the Digital Safety Act. It adds the words "and Data Protection" to the definition of "Commission" and changes the definition of "personal information" to refer to section 2(1) of the PPCDA rather than to section 3 of the *Privacy Act*.

2.2.8 Factors to be Taken into Account when Making Regulations and Issuing Guidelines, Codes of Conduct and Other Documents for the Purposes of the Digital Safety Act (Clause 17 of Bill C-36)

Clause 17 amends section 18(c) of the Digital Safety Act, which states that privacy rights are one of the factors that the Commission must take into account when making regulations and issuing guidelines, codes of conduct and other documents for the purposes of this Act. The amendment adds "and, to the extent it considers appropriate," the purpose of the PPCDA (see section 2.1.2 of this legislative summary).

2.2.9 Repeal of Section 122 of the Digital Safety Act (Clause 18 of Bill C-36)

Clause 18 repeals section 122 of the Digital Safety Act, which requires the Commission and the Privacy Commissioner of Canada to consult with each other in carrying out their respective mandates. It also requires the Commission to consult the Privacy Commissioner of Canada before issuing guidelines, including those relating to age-verification or age-estimation measures, or making regulations, and to take their recommendations into account.

These consultation requirements are being eliminated because Bill C-36 transfers responsibility for PPCDA to the Commission. The Privacy Commissioner of Canada will no longer have a role to play with respect to privacy in the private sector should Bill C-36 be adopted and in force.

PRELIMINARY VERSION
UNEDITED

2.3 PROTECTING PRIVACY AND CONSUMER DATA ACT (CLAUSE 1 OF BILL C-36, SECTIONS 76 TO 147 OF THE PPCDA)

Part 2 of the PPCDA deals with the Commission established by section 4 of the Commission Act, as enacted by Bill C-34 and amended by Bill C-36. It also deals with the Privacy and Consumer Data Commissioner (the Commissioner), as designated under section 85(1) of the PPCDA, and with the Privacy and Consumer Data Division (the Division) established under section 89 of the PPCDA.

The Personal Information and Data Protection Tribunal Act that Bill C-27 sought to enact would have established an administrative tribunal. The administrative tribunal would have heard appeals of certain decisions made by the Privacy Commissioner of Canada under the CPPA (Bill C-27) and would have been able to impose penalties for the contravention of certain provisions of that Act. Many of the powers, duties and functions given to that administrative tribunal under Bill C-27 are now being given to the Commission by Bill C-36. The powers, duties and functions that were given to the Privacy Commissioner of Canada are now given to the Commissioner. This new Commissioner is a member of the Commission, whereas the Privacy Commissioner of Canada is an independent officer of Parliament.[45]

2.3.1 The Digital Safety and Data Protection Commission of Canada (Sections 76 to 84 of the PPCDA)

As part of the powers, duties and functions of the Commission, section 76 of the PPCDA states that the Commission may:

- disclose certain information to the Commissioner of Competition;
- consult with federal government institutions respecting codes of practice or certification programs;
- develop and conduct information programs to foster public understanding of the PPCDA and its purposes;
- develop guidance materials and tools for organizations in relation to their compliance with the PPCDA, including any guidance materials and tools that are requested by the minister, in consultation with stakeholders, including any relevant federal government institutions; and
- promote, by any other means that the Commission considers appropriate, the purpose of the PPCDA.

Section 77 of the PPCDA sets out a non-exhaustive list of relevant factors that the Commission must take into account in exercising any powers or performing any duties or functions under the Act. These factors include the purpose of the PPCDA, the size and revenue of organizations, the best interests of children and the importance of respecting Canada's international trade obligations.

Section 78 of the PPCDA states that the Commission must make readily available information on the manner in which it, the Commissioner and the Division exercise their powers and perform their duties and functions under the Act. It also states that the Commission must develop, in consultation with the minister and stakeholders, guidance material respecting the exercise or performance of the powers, duties and functions in relation to enforcement and dispute resolution under the PPCDA.

Section 79 of the PPCDA states that the Commission may enter into an agreement or arrangement with the minister that relates to the administration of the Act. Section 80 states that it may enter into agreements or arrangements with the Canadian Radio-television and Telecommunications Commission (CRTC), the Commissioner of Competition or any other prescribed entity. The purpose of such agreements or arrangements must be to coordinate the activities of their respective offices, undertake and publish research on issues of mutual interest, and develop procedures for disclosing information relevant to the powers, duties and functions of the Commission, the CRTC, the Commissioner of Competition or the prescribed entity. Section 80 states that the procedures must restrict the use of the information to the purpose for which it was originally disclosed by the Commission and must stipulate that the information be treated in a confidential manner and that it not be further disclosed without the express consent of the Commission.

Section 81 of the PPCDA states that, if the Commission considers it appropriate to do so, or on request by an interested person, the Commission may, in order to ensure that personal information is protected in as consistent a manner as possible, consult with any person who, under provincial legislation, has powers, duties and functions similar to its own, to those of the Commissioner or to those of the Division with respect to the protection of personal information. The Commission may enter into agreements or arrangements with that person in order to coordinate the activities of their respective offices; undertake and publish research, or develop and publish guidelines or other documents, related to the protection of personal information; develop model contracts or other documents related to the protection of personal information that is collected, used or disclosed interprovincially or internationally; and develop procedures for disclosing such information.

The Commission may disclose information to any person who, under provincial legislation, has powers, duties and functions similar to its own, to those of the

Commissioner or to those of the Division with respect to the protection of personal information. The disclosure is permitted if the information in question:

- could be relevant to the investigation of a complaint, proceeding in respect of an application for review or representations to the Commission (under section 109), proceeding in respect of an interim order (under section 123(4)) or audit carried out under the PPCDA or provincial legislation that has objectives that are similar to the PPCDA; or
- could assist that person, the Commission, the Commissioner or the Division in the exercise of their powers or the performance of their duties or functions with respect to the protection of personal information.

The procedures must restrict the use of the information to the purpose for which it was originally disclosed and stipulate that the information be treated in a confidential manner and that it not be further disclosed without the express consent of the Commission.

Under section 82 of the PPCDA, the Commission may disclose certain information to any person or body that, under the legislation of a foreign state, has powers, duties and functions similar to those of the Commission, Commissioner or Division with respect to the protection of personal information or has responsibilities that relate to conduct that is substantially similar to conduct that would be in contravention of the PPCDA. The Commission is authorized to disclose information that it believes:

- could be relevant, according to the Commission, to an investigation or proceeding in respect of a contravention of the laws of a foreign state that address conduct that is substantially similar to conduct that would be in contravention of the PPCDA; or
- is necessary to disclose in order to obtain from the person or body information that could be relevant to an investigation, proceeding in respect of an application referred to in section 109, proceeding in respect of an interim order (under section 123(4)) or audit carried out under the PPCDA.

The Commission may disclose this information only if the Commission has entered into a written arrangement with the person or body that:

- limits the disclosure of information to what is necessary for the purpose for which it was originally disclosed;
- restricts the use of the information to the purpose for which it was originally disclosed; and
- stipulates that the information be treated in a confidential manner and that it not be further disclosed without the express consent of the Commission.

The Commission may also enter into arrangements with one or more persons or bodies representing a foreign state, as described above, in order to:

- provide for cooperation with respect to the enforcement of laws protecting personal information;
- develop procedures for disclosing information that the Commission is authorized to disclose;
- develop recommendations, resolutions, rules, standards or other documents with respect to the protection of personal information;
- undertake and publish research related to the protection of personal information;
- share knowledge and expertise by different means, including through staff exchanges; and
- identify issues of mutual interest and determine priorities pertaining to the protection of personal information.

Section 21(1) of the Commission Act states that the Commission must, within three months after the end of each fiscal year, submit to the minister a report on its activities in that fiscal year. Section 83(1) of the PPCDA adds that the Commission must include in the annual report information in respect of:

- the exercise of the powers, and the performance of the duties and functions, of the Commission, the Commissioner and the Division under the PPCDA;
- the application of the PPCDA; and
- the extent to which the provinces have enacted legislation that is substantially similar to the PPCDA and the application of any such legislation.

Section 83(2) states that the Commission must consult with persons in the provinces who it believes are in a position to assist it in making a report on personal information that is collected, used or disclosed interprovincially or internationally.

Under section 84 of the PPCDA, the Commission may delegate, subject to any terms and conditions that it may specify, to any of its members, the Division or a division of the Commission any of the powers, duties and functions conferred on it under the PPCDA or the Commission Act, to the extent that those powers are exercised and those duties and functions are performed in connection with powers, duties and functions under the PPCDA. However, the Commission must not delegate its power to establish rules respecting its procedures and practices (referred to in section 9 of the Commission Act) in connection with matters to which the PPCDA applies, except to the Commissioner or to the Division. In addition, the Commission must not delegate certain specified powers, duties and functions except to a division of the Commission or to one or more members of the Commission other than the Commissioner.

PRELIMINARY VERSION
UNEDITED

2.3.2 The Privacy and Consumer Data Commissioner (Sections 85 to 88 of the PPCDA)

The Governor in Council must designate one of the members of the Commission, other than the Chairperson, to be the commissioner (section 85 of the PPCDA). As part of the Commissioner's powers, duties and functions, he may:

- request that an entity that operates an approved certification program provide the Commissioner with information that relates to the program;
- cooperate with an entity that operates an approved certification program; and
- in the circumstances and according to the criteria set out in the regulations, recommend to an entity that operates an approved certification program that an organization's certification be withdrawn if the Commissioner is of the opinion that the organization is not in compliance with the requirements of the program, or revoke an approval of a certification program.

Section 86 of the PPCDA provides a non-exhaustive list of relevant factors that the Commissioner must take into account in exercising any powers or performing any duties or functions under the PPCDA. These factors include the purpose of the PPCDA, the size and revenue of organizations, the best interests of children and the importance of respecting Canada's international trade obligations.

The Commissioner must not use the information that the Commission receives in relation to the policies, practices and procedures that are included in an organization's privacy management program (program) as grounds to initiate a complaint or to carry out an audit (section 87 of the PPCDA). However, the Commissioner may use this information if the Commissioner considers that the organization has willfully disregarded the corrective measures that were recommended in relation to its program.

Under section 88 of the PPCDA, the Commissioner may delegate, subject to any terms and conditions that they may specify, certain powers, duties and functions to any employee of the Commission and, with the consent of the Chairperson, to the Division, a division of the Commission or one or more other members of the Commission.

2.3.3 The Privacy and Consumer Data Division (Sections 89 to 91 of the PPCDA)

Section 89 of the PPCDA establishes the Division, which is composed of the Commissioner and at least one other member of the Commission assigned by the Commission. The members who compose the Division (other than the Commissioner) may continue to exercise any power and perform any duty or function that they are authorized to exercise or perform under any other Act of Parliament.

PRELIMINARY VERSION
UNEDITED

Section 90 of the PPCDA sets out a non-exhaustive list of relevant factors that the Division must take into account in exercising any powers or performing any duties or functions under the Act. These factors include the purpose of the PPCDA, the size and revenue of organizations, the best interests of children and the importance of respecting Canada's international trade obligations.

Under section 91 of the PPCDA, the Division may delegate to one or more members of the Commission, or to any of its employees, any of the powers, duties and functions conferred on the Division, subject to any terms and conditions that it may specify. However, the Division must not delegate, without the consent of the Chairperson, any of its powers, duties or functions to a member of the Commission who has not been assigned to the Division.

2.3.4 Codes of Practice and Certification Programs (Sections 92 to 96 of the PPCDA)

For the purposes of sections 92 to 96, the PPCDA states that the term "entity" includes any organization, regardless of whether it is an organization to which the Act applies, or a government institution. Section 92 states that an entity may, in accordance with the regulations, apply to the Division for approval of a code of practice that provides for substantially the same or greater protection of personal information as some or all of the protection provided under the PPCDA. It also states that the Division may approve the code of practice in question if the Division determines that the code meets the criteria set out in the regulations.

Under section 93 of the PPCDA, an entity may, in accordance with the regulations, apply to the Division for approval of a certification program that includes:

- a code of practice;
- guidelines for interpreting and implementing the code of practice;
- a mechanism by which an entity that operates the program may certify that an organization is in compliance with the code of practice;
- a mechanism for the independent verification of an organization's compliance with the code of practice; and
- disciplinary measures for non-compliance with the code of practice by an organization.

The Division may also approve the certification program if the Division determines that the program meets the criteria set out in the regulations.

Section 94 of the PPCDA states that the Division must respond in writing to an application for approval of a code of practice or certification program in the time

PRELIMINARY VERSION
UNEDITED

specified in the regulations. The Division must make public a decision to approve a code of practice or certification program (section 95). Compliance with the requirements of a code of practice or a certification program does not relieve an organization of its obligations under the PPCDA (section 96).

2.3.5 Remedies (Sections 97 to 120 of the PPCDA)

Under section 97 of the PPCDA, an individual may file with the Commissioner a written complaint against an organization for contravening Part 1 of the Act (sections 7 to 75, regarding the obligations of organizations). If the Commissioner is satisfied that there are reasonable grounds to investigate a matter under the PPCDA, the Commissioner may initiate a complaint in respect of the matter (section 97(2)).

A complaint that results from an organization's refusal to grant a request made by an individual to inform them of whether the organization has any personal information about them, how it uses the information and whether it has disclosed the information, and to give the individual access to the information (under section 63) must be filed within six months after the refusal or after the expiry of the time limit for responding to the request, as the case may be. However, the Commissioner may allow any longer period (section 97(3) of the PPCDA). The Commissioner must give notice of a complaint to the organization against which the complaint was made, unless the Commissioner decides, because of an exception under section 99, not to carry out an investigation (section 97(4)).[46]

Section 98(1) states that the Commissioner must carry out an investigation in respect of a complaint unless the Commissioner is of the opinion that:

- the complainant should first exhaust grievance or review procedures otherwise reasonably available;
- the complaint could more appropriately be dealt with by means of a procedure provided for under any federal law (other than the PPCDA) or provincial law;
- the complaint was not filed within a reasonable period;
- the complaint raises an issue in respect of which a certification program that was approved by the Division applies and the organization is certified under that program;
- there is insufficient evidence to pursue the investigation, the complaint is trivial, frivolous or vexatious or is made in bad faith, or the organization has provided a fair and reasonable response to the complaint; or
- the matter is the subject of a compliance agreement entered into under the Act.

PRELIMINARY VERSION
UNEDITED

The Commissioner must notify the complainant and the organization of the Commissioner's decision not to investigate the complaint or any act referred to in the complaint and give reasons for the decision unless the decision is made on the grounds of the exception set out in section 99 (section 98(2)). The Commissioner may reconsider a decision not to investigate a complaint if the Commissioner is satisfied that the complainant has established that there are compelling reasons to investigate (section 98(3)).

The Commissioner may discontinue the investigation of a complaint if the Commissioner has formed an opinion referred to in section 98(1) or is of the opinion that an exception set out in section 99 applies. The Commissioner must notify the complainant and the organization of the discontinuance and give reasons for the decision unless the decision is made on the grounds of the exception set out in section 99 (section 100 of the PPCDA).

Under section 101 of the PPCDA, the Division may attempt to resolve a complaint by means of a dispute resolution mechanism such as mediation and conciliation, unless the complaint is the subject of proceedings in respect of an application referred to in section 109.

If, at any time after an investigation has been commenced, the Commissioner believes on reasonable grounds that an organization has committed, is about to commit or is likely to commit an act or omission that could constitute a contravention of Part 1 of the PPCDA, the Commissioner may enter into, with that organization, a compliance agreement aimed at ensuring compliance with the Act (section 102). A compliance agreement may contain any terms that the Commissioner considers necessary to ensure compliance with the PPCDA (section 102(2)). The Commissioner must not issue a notice of contravention in respect of any matter covered under the compliance agreement. However, entering into a compliance agreement does not preclude the prosecution of an offence under the PPCDA (sections 102(3) and 102(4)).

If, after a notice of contravention has been served on an organization (under section 105(1)), the Commissioner initiates negotiations to enter into a compliance agreement with the organization, the Commission must suspend proceedings in respect of the contravention in relation to the act or omission that is the subject of the negotiations and notify the complainant and the organization without delay. If a compliance agreement is entered into with the organization, the Commission must terminate the proceedings commenced in respect of the contravention in relation to the act or omission that is the subject of the negotiations and notify the complainant and the organization without delay. If the Commissioner and the organization fail to enter into a compliance agreement, the Commission must

PRELIMINARY VERSION
UNEDITED

resume the proceedings and notify the complainant and the organization without delay (section 103 of the PPCDA).

If, after concluding their investigation, the Commissioner decides not to issue a notice of contravention to the organization, the Commissioner must notify the complainant and the organization of their decision and the reasons for it (section 104 of the PPCDA). After investigating a complaint, the Commissioner must cause to be served on the organization a notice of contravention if they have reasonable grounds to believe that the organization has contravened any provision of the PPCDA, and the complaint is not the subject of dispute resolution (under section 101) and has not been resolved or discontinued. The Commissioner must notify the complainant of their decision (section 105).

If the Commissioner has reasonable grounds to believe that an organization is not complying with the terms of a compliance agreement (entered into under section 102), they must cause a notice of contravention to be served on the organization (section 106 of the PPCDA). Section 107 of the PPCDA lists the information that must be set out in the notice of contravention served under section 105. The Commissioner must notify the complainant that the notice of contravention was served and that they may apply for a review and make representations to the Commission.

Under section 107(3) of the PPCDA, the Commissioner may, if they consider it reasonably necessary to ensure compliance with the PPCDA, propose that the Commission order the organization to:

- take any measure necessary in order to comply with the Act or cease any act that contravenes it; and
- make public anything done or planned to be done to correct policies, practices or procedures that the organization put in place to comply with its obligations under the Act.

The organization is deemed to have contravened the provisions at issue if:

- the organization pays the penalty set out in the notice of contravention (section 107(4));
- the organization does not pay the penalty, or neither the complainant nor the organization exercise the remedies referred to in section 109 (section 107(5)); or
- neither the complainant nor the organization exercise the remedies referred to in section 109 in relation to a proposed order (section 107(6)).

PRELIMINARY VERSION
UNEDITED

These presumptions apply, subject to the suspension of proceedings in respect of the contravention of the PPCDA that is the subject of negotiations to enter into a compliance agreement (under section 103). In addition, the proposed order, if any, is made by the Commission and proceedings in respect of those provisions are ended. In all cases, the Commission must notify the complainant of the deemed contravention (section 107 of the PPCDA).

Section 108 lists the information that must be set out in the notice of contravention served under section 106 for non-compliance with a compliance agreement, including the facts of the alleged non-compliance by the organization and the Commissioner's reasons for believing there is non-compliance, as well as the proposed order, if any, that the Commissioner considers reasonably necessary to ensure compliance with the PPCDA. The Commissioner must notify the complainant that the notice of contravention was served and that they may apply for a review and make representations to the Commission (under section 109) within the period set out in that notice.

The Commissioner may, if they consider it reasonably necessary to ensure compliance with the PPCDA, propose that the Commission order the organization to:

- take any measure necessary in order to comply with the PPCDA or cease any act that contravenes it;
- comply with the compliance agreement that the organization entered into; and
- make public anything done or planned to be done to correct policies, practices or procedures that it put in place to comply with its obligations under the PPCDA.

The organization is deemed to have contravened the provisions at issue if:

- the organization pays the penalty set out in the notice of contravention (section 108(4));
- the organization does not pay the penalty, or neither the complainant nor the organization exercise the remedies referred to in section 109 (section 108(5)); or
- neither the complainant nor the organization exercise the remedies referred to in section 109 in relation to a proposed order (section 108(6)).

In addition, as applicable, the organization is liable to pay the penalty set out in the notice, the proposed order is made by the Commission and proceedings in respect of those provisions are ended. In all cases, the Commission must notify the complainant of the deemed contravention.

Under section 109 of the PPCDA, within the period set out in the notice of contravention, the complainant and the organization on which the notice was served

PRELIMINARY VERSION
UNEDITED

may apply for a review of any determination in relation to the elements of a notice in respect of an investigation of a complaint or a compliance agreement (referred to in sections 107(1)(a) to 107(1)(d) or 108(1)(a) to 108(1)(d)), as the case may be, and may make representations to the Commission in accordance with the notice. The Commission may conduct a hearing for the purpose of determining an application and may hold all or any part of the hearing in private. In conducting such proceedings, the Commission must deal with the matters as informally and expeditiously as the circumstances and considerations of fairness and natural justice permit and is not bound by any legal or technical rules of evidence. In addition, the Commission must determine whether the organization committed the contravention on a balance of probabilities.

After considering any representations, the Commission may confirm, cancel or vary any determination that is the subject of proceedings under section 109(1), may decide whether or not to make the order, if any, proposed by the Commissioner and may vary its content before making it (section 110). The Commission may also, to the extent it is reasonably necessary to do so in order to ensure compliance with the PPCDA, order the organization to:

- take any measure necessary in order to comply with the PPCDA or cease any act that contravenes it;
- comply with the compliance agreement that the organization entered into; and
- make public anything done or planned to be done to correct policies, practices or procedures that it put in place to comply with its obligations under the PPCDA.

If the Commission decides that the organization did not commit the contravention, the proceedings in respect of it are ended. The Commission must send a copy of the decision and the reasons for it to the complainant and the organization without delay (section 110(3))[47].

The Commissioner does not have jurisdiction to hear an application referred to in section 109. If a member of the Commission who is assigned to hear, or is hearing, an application referred to in section 109 holds any pecuniary or other interest that could be inconsistent with the proper performance of their duties and functions in relation to the application, the member must disclose the interest to the Chairperson without delay. The member must do the same if their participation could result in a reasonable apprehension of bias (section 111).

The Commission is responsible for making rules respecting the conduct of proceedings in respect of an application referred to in section 109, including the rules of evidence to be followed, and must make those rules publicly available (section 112).

PRELIMINARY VERSION
UNEDITED

Section 113 lists provisions for which a penalty may be imposed if an organization contravenes them. It also lists factors that must be taken into account in determining the amount of a penalty, including the nature and scope of the contravention, any evidence that the organization exercised due diligence to avoid the contravention, and whether the organization made reasonable efforts to mitigate or reverse the contravention's effects. It also states that a penalty must not be imposed if:

- at the time of the contravention, the organization was in compliance with the requirements of a certification program that was in relation to that provision and was approved by the Division;
- a prosecution for the act or omission that constitutes the contravention has been instituted against the organization; or
- the organization establishes that it exercised due diligence to prevent the contravention.

The maximum penalty for all of the contraventions found to have been committed by an organization following the completion of proceedings in relation to any one investigation is the greater of $10 million and 3% of the organization's gross global revenue in its financial year before the one in which the penalty is imposed. The purpose of a penalty is to promote compliance with the PPCDA and not to punish (section 114).

Section 116 sets out the terms and conditions for penalties considered debts due to His Majesty that are payable and that may be recovered by the minister in the Federal Court. No proceedings to recover such a debt may be commenced more than five years after the day on which the debt becomes payable.

The Commissioner may, on reasonable notice and at any reasonable time, carry out an audit of 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 PPCDA (section 118 of the PPCDA). In the course of carrying out an audit, the Commissioner may require the audited organization to cause to be prepared a report, by a third party (that is approved by the Commissioner), on any matter that the Commissioner specifies relating to the organization's compliance with Part 1 and to submit the report to the Commissioner within the time specified by the Commissioner (section 119 of the PPCDA). After carrying out an audit, the Commissioner must provide the audited organization with a report that contains their findings and recommendations, which may be included in the Commission's annual report, under section 21 of the Commission Act and section 83 of the PPCDA (section 120).

PRELIMINARY VERSION
UNEDITED

2.3.6 Powers of the Commission and Commissioner: Investigations, Audits and Proceedings (Sections 121 to 125 of the PPCDA)

In the course of proceedings in respect of an application referred to in section 109, the Commission may, in exigent circumstances, make any interim order that the Commission considers appropriate (section 121). Section 121(2) of the PPCDA lists the powers that the Commission may exercise in the course of proceedings in respect of this application or an interim order (under section 123(4)). For example, the Commission may:

- summon and enforce the appearance of persons before the Commission and compel them to give evidence and to produce any records and things that the Commission considers necessary for the purposes of the proceedings, in the same manner and to the same extent as a superior court of record;
- receive and accept any evidence and other information that the Commission sees fit, whether or not it is or would be admissible in a court of law; and
- enter any premises, other than a dwelling-house, occupied by an organization, converse in private with any person in any premises entered and make any inquiries in those premises that the Commission sees fit, and examine or obtain copies of, or extracts from, records that are found in any premises entered and that contain any matter relevant to the proceedings.

Section 122 lists the powers that the Commissioner may exercise in carrying out an investigation of a complaint or an audit, such as:

- summon and enforce the appearance of persons before the Commissioner and compel them to give evidence and to produce any records and things that the Commissioner considers necessary to carry out the investigation or audit, in the same manner and to the same extent as a superior court of record;
- receive and accept any evidence and other information that the Commissioner sees fit, whether or not it is or would be admissible in a court of law;
- in exigent circumstances, issue a notice of proposed interim order; and
- enter any premises, other than a dwelling-house, occupied by an organization, converse in private with any person in any premises entered and make any inquiries in those premises that the Commissioner sees fit, and examine or obtain copies of, or extracts from, records found in any premises entered that contain any matter relevant to the investigation or audit.

Section 122(3) lists the information that must be included in a notice of proposed interim order (referred to in section 122(1)(d)), specifically the proposed interim order and the reasons for it, the right of the organization and of the complainant

PRELIMINARY VERSION
UNEDITED

to make representations to the Commission and the procedure for doing so, and the fact that, if representations are not made in accordance with the notice, the proposed order will be imposed.

The complainant and the organization may make representations to the Commission within the period set out in the notice of proposed interim order and in accordance with that notice. The Commission may conduct a hearing for the purpose of considering the proposed interim order and the reasons for it and may hold all or any part of the hearing in private. In conducting such proceedings, the Commission is not bound by any legal or technical rules of evidence and must deal with the matter as informally and expeditiously as the circumstances and considerations of fairness and natural justice permit. After considering the representations, the Commission must decide, on a balance of probabilities, whether or not to make the interim order. The Commission may also vary the content of the proposed interim order. The Commission must send a copy of the decision and its reasons to the complainant and the organization without delay (section 123).

If neither the complainant nor the organization make representations to the Commission within 10 days after the day on which the notice is served, or within any further period set out in the notice (under section 122(3)(c)), the proposed interim order "as is" is made by the Commission (section 123(6) of the PPCDA).

If a member of the Commission who is assigned to hear, or is hearing, proceedings in respect of representations from the complainant and the organization regarding the notice of proposed interim order (under section 123(1)) holds any pecuniary or other interest that could be inconsistent with the proper performance of their duties and functions in relation to the proceedings, the member must disclose the interest to the Chairperson without delay (section 124 of the PPCDA). The member must also disclose, without delay, any reason why their participation could result in a reasonable apprehension of bias. The Commissioner does not have jurisdiction to hear proceedings referred to in section 123(1).

The Commission is responsible for making rules respecting the conduct of proceedings in respect of representations from the complainant and the organization regarding the notice of proposed interim order (under section 123(1)), including the rules of evidence to be followed, and must make those rules publicly available (section 125 of the PPCDA).

2.3.7 Appeals
(Sections 126 to 128 of the PPCDA)

Section 126 of the PPCDA specifies the decisions and orders that an affected complainant or organization may appeal to the Federal Court. The time limit for making an appeal is 30 days after the day on which the Commission makes a decision on an

PRELIMINARY VERSION
UNEDITED

application for review or representations made to the Commission by the complainant and the organization in respect of an investigation of a complaint or a compliance agreement (under section 110(1)).

A complainant or organization that is affected by an interim order (made under section 121 or 123(4)) may, with leave of the Federal Court, appeal the order to the Federal Court (section 127 of the PPCDA). The time limit for making an application for leave to appeal is 30 days after the day on which the order is made. The Federal Court may dispose of an appeal by dismissing it or by allowing it and, in allowing the appeal, the Federal Court may substitute its own finding, order or decision for the one under appeal or may refer the matter back to the Commission for reconsideration (section 128 of the PPCDA).

2.3.8 Enforcement of Orders (Sections 129 to 131 of the PPCDA)

Under section 129 of the PPCDA, an order made by the Commission may, for the purpose of its enforcement, be made an order of the Federal Court if a presumption applies to a notice of contravention for the investigation of a complaint or a compliance agreement (under section 107(4), 107(5) or 107(6), or 108(4), 108(5) or 108(6) of the PPCDA). The order is enforceable in the same manner as an order of the Federal Court.

An order may also, for the purpose of its enforcement, be made an order of the Federal Court and be enforceable in the same manner as an order of that Court if the order is made by the Commission with regard to an application for review or representations made to the Commission by the complainant and the organization in respect of an investigation of a complaint or a compliance agreement (under section 110(1)) and is not appealed to the Federal Court or an appeal of the order is dismissed by the Federal Court.

The same solution applies if an application for leave to appeal an interim order made by the Commission (under section 121(1) or 123(4)) to the Federal Court is not made, a leave application in relation to the order is dismissed by the Federal Court or the application for leave in relation to the order is granted by the Federal Court but the appeal is dismissed.

The Federal Court may, in accordance with its rules, award costs. However, no costs may be awarded against the Commission unless the Federal Court is satisfied that an award is necessary to maintain the public's confidence in the administration of justice, or that the absence of an award would have a substantial adverse effect on the other party's ability to carry on business (section 131 of the PPCDA).

PRELIMINARY VERSION
UNEDITED

2.3.9 Private Right of Action (Section 132 of the PPCDA)

Section 132 of the PPCDA states that an individual who suffers loss or injury as a result of an act or omission by an organization that constitutes a contravention of the Act has a cause of action against the organization for damages. It lists the conditions that must be met for this private right of action to be available. They include the fact that the Commissioner has made a finding that the organization has contravened the PPCDA (under the specified circumstances) or that the Federal Court has dismissed an appeal or made a finding that the organization has contravened the Act pursuant to section 128.

Section 132(2) also states that an individual who suffers loss or injury as a result of an act or omission by an organization that has been convicted of an offence under section 145 of the PPCDA has a cause of action against the organization for damages. This private right of action does not limit or affect an individual's right to avail themselves of a civil remedy under another Act of Parliament, under an Act of a legislature of a province or at common law (section 132(3)).

An action must not be brought later than two years after the day on which the individual becomes aware of the relevant facts, as specified in the provision, and it may be brought in the Federal Court or a superior court of a province (sections 132(4) and 132(5) of the PPCDA).

2.3.10 Certificate Under the *Canada Evidence Act* (Sections 133 to 138 of the PPCDA)

There are certain situations where a certificate under the *Canada Evidence Act* (section 38.13 or 38.41) interacts with the PPCDA (section 133 of the PPCDA). If a certificate prohibiting the disclosure of personal information of a specific individual is issued *before* a complaint is filed by that individual under the PPCDA in respect of a request for access to his personal information, that individual does not have the right to access that information. If a certificate prohibiting the disclosure of personal information is issued *after* the filing of such a complaint under the PPCDA, all proceedings under the PPCDA in respect of that information are discontinued (section 133 of the PPCDA).

In all cases, the Commission, the Commissioner and the Division and every person acting on their behalf or under their direction must not disclose information subject to the certificate and must take every reasonable precaution to avoid the disclosure of that information (section 133(3) of the PPCDA). This section also sets out the conditions under which the Commissioner or the Commission, as the case may be, may delegate the investigation in respect of any complaint, the consideration of an application for a review (under section 109) or a proceeding in respect of an interim

PRELIMINARY VERSION
UNEDITED

order (referred to in section 123(4)) that is in relation to information subject to a certificate (sections 133(4) and 133(5)).

Sections 134 and 135 set out the manner in which the Commission, the Commissioner and the Division, and any person acting on their behalf or under their direction must satisfy any applicable security and secrecy requirements with respect to confidential information. However, section 135(3) of the PPCDA provides that the Commission, the Commissioner or the Division may make public any information if they consider that it is in the public interest to do so. In addition, they may disclose or may authorize any person acting on their behalf or under their direction to disclose, information that in their opinion is necessary for the exercise of any of their powers or the performance of any of their duties or functions or for certain judicial proceedings (section 135(5)).

They may also disclose to the Attorney General of Canada or of a province, as the case may be, information relating to the commission of an offence under any federal or provincial law on the part of an officer or employee of an organization if, in their opinion, there is evidence of an offence (section 135(6)).

In addition, they may disclose, or may authorize any person acting on their behalf or under their direction to disclose, to a government institution or a part of a government institution, any information contained in a report made to the Commission of any breach of security safeguards that creates a real risk of significant harm to an individual (under section 58(1)) or in a record of every breach of security safeguards involving personal information under an organization's control (under section 60(2)) if they have reasonable grounds to believe that the information could be useful in the investigation of a contravention of any federal or provincial law that has been, is being or is about to be committed (section 135(7)).

Lastly, they may disclose, or may authorize any person acting on their behalf or under their direction to disclose, information in accordance with section 58(3) or 60(1) of Canada's anti-spam legislation (section 135(8) of the PPCDA).[48]

Section 136 of the PPCDA lists the proceedings in which the Commission, the Commissioner or the Division, or any person acting on their behalf or under their direction is a competent witness in respect of any matter that comes to their knowledge as a result of the exercise of any of their powers or the performance of any of their duties or functions under the Act.

No criminal or civil proceedings lie against the Commission, the Commissioner or the Division, or against any person acting on their behalf or under their direction, for anything done, reported, decided or said in good faith as a result of the exercise or purported exercise of any of their powers or the performance or purported performance

PRELIMINARY VERSION
UNEDITED

of any of their duties or functions under the PPCDA. They also have immunity against actions in defamation (section 137 of the PPCDA).

For the purposes of section 75(i) of the PPCDA, which sets out an exception to the prohibition on any organization using de-identified personal information to identify an individual, the Division may, on request by an organization, authorize a purpose or situation in which the organization may use de-identified personal information in this manner, if it is clearly in the individual's interest (section 138 of the PPCDA).

2.3.11 General (Sections 139 to 146 of the PPCDA)

Section 139 of the PPCDA provides a non-exhaustive list of purposes for which the Governor in Council may make regulations for carrying out the purposes and provisions of the Act. These purposes include:

- respecting the anonymization of personal information;
- respecting the scope of the business activities for the purpose of which an organization may collect or use an individual's personal information without their knowledge or consent (under sections 18(2)(a) to 18(2)(c));
- specifying activities that are not business activities for the purposes of section 18(1); and
- respecting an individual's right of access to their personal information.

It also sets out what the Governor in Council may do by order. For instance, the Governor in Council may, if satisfied that legislation of a province that is substantially similar to the PPCDA applies to an organization, a class of organizations, an activity or a class of activities, exempt the organization, activity or class from the application of the PPCDA in respect of the collection, use or disclosure of personal information that occurs within that province. The Governor in Council may also make regulations establishing criteria that are to be applied in making a determination that provincial legislation is substantially similar to the PPCDA (under section 139(2)(b)) or in reconsidering that determination and the process for making or reconsidering that determination.

In addition, the Governor in Council may make regulations respecting the disclosure of personal information in relation to a data mobility framework established under section 72. This may include regulations providing for exceptions to the requirement to disclose personal information, including exceptions related to the protection of proprietary or confidential commercial information (section 140).

Section 142 states that the minister may make regulations respecting codes of practice and certification programs, including the circumstances in which the Commissioner may

recommend that an organization's certification be withdrawn (under section 85(2)(c)) or in which an approval of a certification program may be revoked (under section 85(2)(d)).

Any person who has reasonable grounds to believe that a person has contravened or intends to contravene Part 1 of the PPCDA may notify the Commission of the particulars of the matter and may request that their identity be kept confidential with respect to the notification (section 143 of the PPCDA). The Commission must keep confidential the identity of a person to whom an assurance of confidentiality has been provided by the Commission.

Under section 144, an employer must not dismiss, suspend, demote, discipline, harass or otherwise disadvantage an employee, or deny an employee a benefit of employment, by reason that the employee, acting in good faith and on the basis of reasonable belief:

- has disclosed to the Commission that the employer or any other person has contravened or intends to contravene Part 1 of the PPCDA;
- has refused or stated an intention of refusing to do anything that is a contravention of Part 1 of the PPCDA; or
- has done or stated an intention of doing anything that is required to be done in order that Part 1 of the PPCDA not be contravened.

This prohibition on reprisal also applies if the employer believes that the employee will do any of the above. Nothing in this provision impairs any right of an employee, either at law or under an employment contract or collective agreement. The definition of "employee" includes an independent contractor, and the definition of "employer" has a corresponding meaning.

Section 145 describes what constitutes an offence under the PPCDA and states that if the organization is guilty of an indictable offence, it is liable to a fine not exceeding the greater of $25 million and 5% of the organization's gross global revenue in its financial year before the one in which the organization is sentenced. If the organization is guilty of an offence punishable on summary conviction, it is liable to a fine not exceeding the greater of $20 million and 4% of the organization's gross global revenue in its financial year before the one in which the organization is sentenced. The fine is imposed following prosecution, not by the Commission.

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 is $100,000.

Section 146 provides for a parliamentary review of the PPCDA every five years following the coming into force of that provision.

PRELIMINARY VERSION
UNEDITED

2.3.12 Coming into Force (Section 147 of the PPCDA)

Section 147 of the PPCDA states that the provisions of the Act come into force on a day or days to be fixed by order of the Governor in Council, but that day or those days must not be before the day on which Part 3 of Bill C-36, which deals with the Commission, comes into force. In short, the PPCDA may not come into force until the Commission is established and made responsible for exercising the powers and performing the duties and functions conferred on it under that Act. Until then, PIPEDA remains in force, and the Privacy Commissioner of Canada continues to oversee compliance with it.

2.4 AMENDMENT TO THE *PERSONAL INFORMATION PROTECTION AND ELECTRONIC DOCUMENTS ACT* (CLAUSES 2 TO 7 OF BILL C-36)

Clause 2 of the bill replaces the long title of PIPEDA with "An Act to provide for the use of electronic means to communicate or record information or transactions."

Clause 3 replaces sections 1 to 30 of PIPEDA with a new section 1 stating that the short title of the amended Act is the "Electronic Documents Act." Consequently, Part 1 of PIPEDA, which consists of sections 2 to 30, dealing with the protection of personal information in the private sector, is replaced by the PPCDA.

Clause 4 adds a new section 31(3) to PIPEDA, stating that the Governor in Council may, by order, designate a member of the King's Privy Council for Canada as the Minister responsible for the Act.

Clauses 5, 6 and 7 respectively repeal parts 3 to 5, Schedule 1 and Schedule 4 of PIPEDA. Parts 3 to 5 set out amendments to the *Canada Evidence Act*, the *Statutory Instruments Act* and the *Statute Revision Act*. Schedule 1 sets out the "Principles Set Out in the National Standard of Canada Entitled Model Code for the Protection of Personal Information, CAN/CSA-Q830-96," to which section 5 of PIPEDA refers and which represent the basis of the obligations under PIPEDA.

Schedule 4 simply lists the World Anti-Doping Agency as an organization to which sections 4(1.1) and 26(2)(c) of PIPEDA refer, with respect to "personal information that the organization collects, uses or discloses in the course of its interprovincial or international activities." These provisions state that Part 1 of PIPEDA applies to organizations set out in Schedule 4 in respect of personal information set out in that schedule and that the Governor in Council may, by order, amend that schedule. Schedule 4 to PIPEDA is reproduced in full in the schedule to the PPCDA and is referred to by its sections 6(3) and 139(2)(c).

PRELIMINARY VERSION
UNEDITED

2.5 CONSEQUENTIAL AND RELATED AMENDMENTS, TRANSITIONAL PROVISION, COORDINATING AMENDMENTS AND COMING INTO FORCE (CLAUSES 26 TO 52 OF BILL C-36)

Clauses 26 to 49 make consequential and related amendments to other Acts to refer to the PPCDA rather than to PIPEDA.[49] They also replace certain references to the Privacy Commissioner of Canada with the Privacy and Consumer Data Commissioner, Commission and Division or add those entities to the appropriate provisions.

The bill amends the *Canadian Radio-television and Telecommunications Commission Act* and the *Competition Act* to confer on the CRTC and the Commissioner of Competition the power to enter into an agreement or arrangement with the Commission and to develop procedures for disclosing information to the Commission (clauses 30 and 31). It also amends the *Broadcasting Act* and the *Telecommunications Act* to authorize the CRTC to disclose information designated as confidential to the Commission (clauses 34 and 35).

Clause 49 makes terminology changes to 13 Acts to replace PIPEDA with "Electronic Documents Act."[50] Clause 50 states that the Governor in Council may make regulations respecting any transitional matter arising from the coming into force of the provisions of the PPCDA.

Clause 51 sets out certain coordinating amendments. It states that if clause 3 of Bill C-36 (which replaces sections 1 to 30 of PIPEDA) comes into force before Division 23 of Part 5 of the *Budget 2025 Implementation Act, No. 1* (which adds a new division to PIPEDA regarding mobility of personal information), then that Division 23 is repealed. It also states that if clause 3 of Bill C-36 comes into force on the same day as Division 23 of Part 5 of the *Budget 2025 Implementation Act, No. 1*, then that Division 23 is deemed never to have come into force and is repealed.

Clause 52 states that the provisions of Bill C-36, other than clauses 1 and 51 and Part 3, come into force on a day to be fixed by order of the Governor in Council. Clause 1 enacts the PPCDA and sets out its text, clause 51 sets out the amendments to coordinate Bill C-36 with the *Budget 2025 Implementation Act, No. 1*, and Part 3 deals with the Commission. The day to be fixed by order of the Governor in Council must not be before the day on which that Part 3 comes into force.

If Bill C-34 receives Royal Assent, then Part 3 of Bill C-36 comes into force on a day to be fixed by order of the Governor in Council, but that day must not be before the day on which section 4 of the Commission Act, which establishes the Commission, comes into force.

PRELIMINARY VERSION
UNEDITED

NOTES

1. Bill C-36, An Act to enact the Protecting Privacy and Consumer Data Act, to amend the Personal Information Protection and Electronic Documents Act and to make amendments to other Acts, 45th Parliament, 1st Session. At the time of writing this legislative summary, no *Canadian Charter of Rights and Freedoms* (the Charter) Statement had been tabled in the House of Commons for Bill C-36.

2. This legislative summary incorporates some of the content of the legislative summary of Bill C-27 for the parts of Bill C-36 that are identical or similar, with relevant modifications. See Sabrina Charland, Alexandra Savoie and Ryan van den Berg, *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*, Publication no. 44-1-C27-E, Library of Parliament, 12 July 2022.

3. Bill C-34, An Act to enact the Digital Safety Act and the Digital Safety Commission of Canada Act and to make consequential amendments to other Acts, 45th Parliament, 1st Session.

4. For a more comprehensive history of the *Personal Information Protection and Electronic Documents Act* (PIPEDA) and of the calls for reform made before 2020, see Alexandra Savoie and Maxime-Olivier Thibodeau, *Canada's Federal Privacy Laws*, Publication no. 2007-44-E, Library of Parliament, 17 November 2020. See also Office of the Privacy Commissioner of Canada (OPC), *A pivotal time for privacy: 2021–2022 Annual Report to Parliament on the* Privacy Act *and the* Personal Information Protection and Electronic Documents Act, 2022; House of Commons, Standing Committee on Access to Information, Privacy and Ethics (ETHI), *Oversight of Social Media Platforms: Ensuring Privacy and Safety Online*, Sixteenth report, December 2024; and ETHI, *Facial Recognition Technology and the Growing Power of Artificial Intelligence*, Sixth report, October 2022.

5. 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. See also 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.

6. See 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.

7. 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. See also Government of Canada, *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 – Charter Statement*, 4 November 2022.

8. Sabrina Charland, Alexandra Savoie and Ryan van den Berg, *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*, Publication no. 44-1-C27-E, Library of Parliament, 12 July 2022.

9. House of Commons, Standing Committee on Industry and Technology (INDU), *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*. INDU held more than 30 meetings to study Bill C-27. It heard 137 witnesses and received 116 briefs.

10. Innovation, Science and Economic Development Canada (ISED), *Canada's National Artificial Intelligence Strategy: AI for All*.

11. ISED, "Key pillars of the strategy – Pillar 1: Protecting Canadians and safeguarding our democracy," *Canada's National Artificial Intelligence Strategy: AI for All*.

PRELIMINARY VERSION
UNEDITED

12. Bill C-36 makes no explicit reference to surveillance pricing, a practice where companies use an algorithm to analyze consumers' personal data in order to determine optimal prices for products and services and maximize profits. Some provisions of the Protecting Privacy and Consumer Data Act (PPCDA) could apply to this practice. Algorithmic pricing touches on various areas of law, including competition, privacy, consumer protection and contracts. The latter two areas of law generally fall under provincial jurisdiction over property, civil rights and all matters of a merely local or private nature (*Constitution Act, 1867*, 30 & 31 Victoria, c. 3 [U.K.], ss. 92(13) and 92(16)). In provinces that have passed legislation that is substantially similar to PIPEDA, provincial private-sector privacy laws fall under these two powers. PIPEDA was passed pursuant to Parliament's power to regulate trade and commerce (*Constitution Act, 1867*, 30 & 31 Victoria, c. 3 [U.K.], s. 91(2)).

13. Bill C-11 and Bill C-27 sought to implement Canada's Digital Charter. See ISED, *Canada's Digital Charter*.

14. European Union (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 Trade Commissioner Service, *The European Union's General Data Protection Regulation [GDPR]*.

15. 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.

16. EU, EUR-Lex, *Report from the Commission to the European Parliament and the Council on the first review of the functioning of the adequacy decisions adopted pursuant to Article 25(6) of Directive 95/46/EC*, 15 January 2024. See European Commission, *Adequacy decisions*.

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. Under the GDPR, personal data may be transferred to a third country or an international organization when the European Commission finds that the third party or international organization ensures an adequate level of protection.

18. 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.

19. Kate Sinnott, "Coming into Force of Federal Legislation: A Practical Guide," *HillNotes*, Library of Parliament, 4 October 2022.

20. See, for example, *Johnson v. Bell Canada (F.C.)*, 2008 FC 1086 (CanLII), [2009] 3 F.C.R. 67, para. 21; and *Fahmy v. Bank of Montreal*, 2016 FC 479 (CanLII), para. 49.

21. In PIPEDA, the context in which the rules are established is as follows: "in an era in which technology increasingly facilitates the circulation and exchange of information."

22. OPC, *Submission of the Office of the Privacy Commissioner of Canada on Bill C-27, the* Digital Charter Implementation Act, 2022, April 2023, Recommendation 1.

23. OPC, *PIPEDA requirements in brief*.

24. At this time, Alberta, British Columbia 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 PPCDA is "essentiellement semblable" while the French term used in PIPEDA is "essentiellement similaire." In English, the term "substantially similar" is used in both.

25. Bill C-36, An Act to enact the Protecting Privacy and Consumer Data Act, to amend the Personal Information Protection and Electronic Documents Act and to make amendments to other Acts, 45th Parliament, 1st Session, s. 2.

26. 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 PPCDA. See *A.T. v. Globe24h.com*, 2017 FC 114 (CanLII), [2017] 4 F.C.R. 310, para. 50.

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

28. Section 2 of the PPCDA indicates that sensitive personal information includes a child's personal information, personal information revealing an individual's racial or ethnic origin, political opinions, religious or philosophical beliefs, an individual's trade union membership, genetic information or health information, biometric information that is capable of uniquely identifying the individual or information concerning an individual's sexual orientation.

29. Sections 12 to 14 of the PPCDA reflect the content of Principle 2, Principle 4 and Principle 5 set out in Schedule 1 of PIPEDA. Section 15(7) of the PPCDA 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."

30. *Personal Information Protection and Electronic Documents Act*, S.C. 2000, c. 5, s. 6.1.

31. *Personal Information Protection and Electronic Documents Act*, S.C. 2000, c. 5, s. 7.2.

32. *Proceeds of Crime (Money Laundering) and Terrorist Financing Act*, S.C. 2000, c. 17.

33. Ibid.; *Personal Information Protection and Electronic Documents Act*, S.C. 2000, c. 5, s. 7(3)(c.2); and Protecting Privacy and Consumer Data Act, s. 45.

34. Section 39 of the Consumer Privacy Protection Act (CPPA), which Bill C-27 proposed to create.

35. Under section 7(2) of PIPEDA, an organization may use personal information without the knowledge or consent of the individual if "it is used for statistical, or scholarly study or research, purposes that cannot be achieved without using the information, the information is used in a manner that will ensure its confidentiality, it is impracticable to obtain consent and the organization informs the Commissioner of the use before the information is used."

36. Sections 52 to 55 of the PPCDA reflect the content of Principle 5 and Principle 6 set out in Schedule 1 of PIPEDA, which have to do with limiting the use, disclosure and retention of personal information, as well as the accuracy of that information.

37. Section 54(2) of the CPPA, which Bill C-27 proposed to create.

38. Section 55(2) of the CPPA, which Bill C-27 proposed to create.

39. OPC, *Submission of the Office of the Privacy Commissioner of Canada on Bill C-27, the* Digital Charter Implementation Act, 2022, April 2023, Recommendation 8.

40. This obligation reflects the content of Principle 7 set out in Schedule 1 of PIPEDA, which has to do with safeguards.

41. Section 62 of the PPCDA reflects the content of Principle 8 set out in Schedule 1 of PIPEDA, which has to do with transparency.

42. Bill C-36, An Act to enact the Protecting Privacy and Consumer Data Act, to amend the Personal Information Protection and Electronic Documents Act and to make amendments to other Acts, 45th Parliament, 1st Session, s. 2.

43. OPC, *Submission of the Office of the Privacy Commissioner of Canada on Bill C-27, the* Digital Charter Implementation Act, 2022, April 2023, Recommendation 5.

44. Sections 63 to 71 of the PPCDA reflect the content of Principle 9 set out in Schedule 1 of PIPEDA, which has to do with access to personal information.

45. The mission of the Privacy Commissioner of Canada is to oversee compliance with the federal private-sector privacy law since the passage of PIPEDA in 2000. Many of his investigations in recent years have concerned the private sector, particularly organizations operating in the digital domain.

PRELIMINARY VERSION
UNEDITED

46. Section 99 of the PPCDA states that, despite section 98(1), under which the Commissioner must carry out an investigation in respect of a complaint unless the Commissioner decides not to investigate for any of the listed reasons,

> the Commissioner is not required to carry out an investigation in respect of an act referred to in a complaint if the Commissioner is of the opinion that the act, if proved, would constitute a contravention of any of sections 6 to 9 of *An Act to promote the efficiency and adaptability of the Canadian economy by regulating certain activities that discourage reliance on electronic means of carrying out commercial activities, and to amend the Canadian Radio-television and Telecommunications Commission Act, the Competition Act, the Personal Information Protection and Electronic Documents Act and the Telecommunications Act* or section 52.01 of the *Competition Act* or would constitute conduct that is reviewable under section 74.011 of that Act.

47. Section 110(3) of the PPCDA provides that the Commission must send a copy of the decisions whereas in French the same provision provides that the Commissioner must do so. Considering that section 110 deals with decisions taken by the Commission, the English provision appears to be the correct one.

48. *An Act to promote the efficiency and adaptability of the Canadian economy by regulating certain activities that discourage reliance on electronic means of carrying out commercial activities, and to amend the Canadian Radio-television and Telecommunications Commission Act, the Competition Act, the Personal Information Protection and Electronic Documents Act and the Telecommunications Act*, S.C. 2010, c. 23.

49. The 11 laws it amends are: the *Access to Information Act*, the *Aeronautics Act*, the *Canada Evidence Act*, the *Canadian Radio-television and Telecommunications Commission Act*, the *Competition Act*, the *Canada Business Corporations Act*, the *Railway Safety Act*, the *Broadcasting Act*, the *Telecommunications Act*, the *Public Servants Disclosure Protection Act* and Chapter 23 of the Statutes of Canada (2010).

50. The 13 laws it amends are: the *Canada Evidence Act*, the *Canadian Forces Superannuation Act*, the *Canada Business Corporations Act*, the *Public Service Superannuation Act*, the *Royal Canadian Mounted Police Superannuation Act*, the *Canada–Newfoundland and Labrador Atlantic Accord Implementation and Offshore Renewable Energy Management Act*, the *Canada–Nova Scotia Offshore Petroleum Resources Accord Implementation and Offshore Renewable Energy Management Act*, the *Trust and Loan Companies Act*, the *Bank Act*, the *Insurance Companies Act*, the *Cooperative Credit Associations Act*, the *Canada Cooperatives Act* and the *Canada Not-for-profit Corporations Act*.