

~~Second~~First Session, Forty-~~third~~fourth Parliament,  
~~69~~70-71 Elizabeth II, ~~2020~~2021-2022

HOUSE OF COMMONS OF CANADA

**BILL C-~~11~~27**

An Act to enact the Consumer Privacy Protection Act ~~and~~, 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

**SUMMARY**

Part 1 enacts the *Consumer Privacy Protection Act* to ~~protect~~govern the protection of personal information of individuals while ~~recognizing~~taking into account the need of organizations to collect, use or disclose personal information in the course of commercial activities. In consequence, it repeals Part 1 of the *Personal Information Protection and Electronic Documents Act* and changes the short title of that Act to the *Electronic Documents Act*. It also makes consequential and related amendments to other Acts.

Part 2 enacts the *Personal Information and Data Protection Tribunal Act*, which establishes an administrative tribunal to hear appeals of certain decisions made by the Privacy Commissioner under the *Consumer Privacy Protection Act* and to impose penalties for the contravention of certain provisions of that Act. It also makes a related amendment to the *Administrative Tribunals Support Service of Canada Act*.

Part 3 enacts the *Artificial Intelligence and Data Act* to regulate international and interprovincial trade and commerce in artificial intelligence systems by requiring that certain persons adopt measures to mitigate risks of harm and biased output related to high-impact artificial intelligence systems. That Act provides for public reporting and authorizes the Minister to order the production of records related to artificial intelligence systems. That Act also establishes prohibitions related to the possession or use of illegally obtained personal information for the purpose of designing, developing, using or making available for use an artificial intelligence system and to the making available for use of an artificial intelligence system if its use causes serious harm to individuals.

## TABLE OF PROVISIONS

**An Act to enact the Consumer Privacy Protection Act~~and~~, 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**

### [Preamble](#)

#### Short Title

1 *Digital Charter Implementation Act, ~~2020~~[2022](#)*

#### PART 1

#### Consumer Privacy Protection Act

### [Enactment of Act](#)

2 Enactment

**An Act to support and promote electronic commerce by protecting personal information that is collected, used or disclosed in the course of commercial activities**

#### Short Title

1 *Consumer Privacy Protection Act*

#### Interpretation

2 Definitions

3 Order designating Minister

4 Authorized representatives

#### Purpose and Application

5 Purpose

6 Application

#### PART 1

#### Obligations of Organizations

### **Accountability of Organizations**

- 7 Accountability — personal information under organization's control
- 8 Designated individual
- 9 Privacy management program
- 10 Access ~~by Commissioner — policies, practices and procedures~~ privacy management program
- 11 Same protection

### **Appropriate Purposes**

- 12 Appropriate purposes

### **Limiting Collection, Use and Disclosure**

- 13 Limiting collection
- 14 New purpose

### **Consent**

- 15 Consent required
- 16 Consent obtained by deception
- 17 Withdrawal of consent

### **Exceptions to Requirement for Consent**

#### **Business Operations**

- 18 Business activities
- 19 Transfer to service provider
- 20 De-identification of personal information
- 21 Research, analysis and development

- 22 Prospective business transaction
- 23 Information produced in employment, business or profession
- 24 Employment relationship — federal work, undertaking or business
- 25 Disclosure to lawyer or notary
- 26 Witness statement
- 27 Prevention, detection or suppression of fraud
- 28 Debt collection

### **Public Interest**

- 29 Individual's interest
- 30 Emergency — use
- 31 Emergency — disclosure
- 32 Identification of individual
- 33 Communication with next of kin or authorized representative
- 34 Financial abuse
- 35 ~~Statistical or scholarly~~ [Statistics](#), study or research
- 36 Records of historic or archival importance
- 37 Disclosure after period of time
- 38 Journalistic, artistic or literary purposes
- 39 Socially beneficial purposes

### **Investigations**

- 40 Breach of agreement or contravention
- 41 Use for investigations
- 42 Breach of security safeguards

### **Disclosures to Government Institutions**

- 43 Administering law — request of government institution
- 44 Law enforcement — request of government institution
- 45 Contravention of law — initiative of organization
- 46 *Proceeds of Crime (Money Laundering) and Terrorist Financing Act*
- 47 ~~Request by government institution~~ ~~— national~~ National security, defence or international affairs — request by government institution
- 48 ~~Initiative of organization~~ ~~— national~~ National security, defence or international affairs — initiative of organization

### **Required by Law**

- 49 Required by law — collection
- 50 Subpoena, warrant or order

### **Publicly Available Information**

- 51 Information specified by regulations

### **Non-application of Certain Exceptions — Electronic Addresses and Computer Systems**

- 52 Definitions

### **Retention and Disposal of Personal Information**

- 53 Period for retention and disposal
- 54 Personal information used for decision-making
- 55 Disposal at individual's request

### **Accuracy of Personal Information**

56 Accuracy of information

### **Security Safeguards**

57 Security safeguards

58 Report to Commissioner

59 Notification to organizations

60 Records

61 Service providers

### **Openness and Transparency**

62 Policies and practices

### **Access to and Amendment of Personal Information**

63 Information and access

64 Request in writing

65 Information to be provided

66 Plain language

67 Time limit

68 Costs for responding

69 Retention of information

70 When access prohibited

71 Amendment of personal information

### **Mobility of Personal Information**

72 Disclosure under data mobility framework

## **Challenging Compliance**

73 Complaints and requests for information

## **De-identification of Personal Information**

74 Proportionality of technical and administrative measures

75 Prohibition

## **PART 2**

### **Commissioner's Powers, Duties and Functions and General Provisions**

#### **Codes of Practice and Certification Programs**

76 Definition of entity

77 Certification program

78 Response by Commissioner

79 Approval made public

80 For greater certainty

81 Powers of Commissioner

#### **Recourses**

#### **Filing of Complaints**

82 Contravention

#### **Investigation of Complaints and Dispute Resolution**

83 Investigation of complaint by Commissioner

84 [Exception](#)

[85 Discontinuance](#)

[86](#) Dispute resolution mechanisms

### ~~Discontinuance of Investigation~~

~~85~~ ~~Reasons~~

### Compliance Agreements

[8687](#) Entering into compliance agreement

### Notification

[8788](#) Notification and reasons

### Inquiry

[8889](#) Inquiry — complaint

[8990](#) Inquiry — compliance agreement

[9091](#) Nature of inquiries

~~91~~ ~~Procedure~~

92 Rules

[93](#) Decision

### Administrative Monetary Penalties

[9394](#) Recommendation

[9495](#) Imposition of penalty

[9596](#) Recovery as debt due to Her Majesty

### Audits

[9697](#) Ensure compliance



[9798](#) Report of findings and recommendations

## **Commissioner's Powers — Investigations, Inquiries and Audits**

[9899](#) Powers of Commissioner

[99100](#) Delegation

### **Appeals**

[100101](#) Right of appeal

[101102](#) Appeal with leave

[102103](#) Disposition of appeals

### **Enforcement of Orders**

[103104](#) Compliance orders

[104105](#) Tribunal orders

[105106](#) Filing with Court

### **Private Right of Action**

[106107](#) Damages — contravention of Act

### **Certificate Under Canada Evidence Act**

[107108](#) Certificate under *Canada Evidence Act*

### **Powers, Duties and Functions of Commissioner**

[108109](#) Factors to consider

[109110](#) Promoting purposes of Act

[110111](#) Prohibition — use for initiating complaint or audit

~~111~~[112](#) Information — powers, duties or functions

~~112~~[113](#) Confidentiality

~~113~~[114](#) Not competent witness

~~114~~[115](#) Protection of Commissioner

~~115~~

[116](#) De-identified information

[117](#) Agreements or arrangements — Minister

[118](#) Agreements or arrangements — CRTC and Commissioner of Competition

~~116~~[119](#) Consultations with provinces

~~117~~[120](#) Disclosure of information to foreign state

~~118~~[121](#) Annual report

## **General**

~~119~~[122](#) Regulations

~~120~~[123](#) Data mobility frameworks

~~121~~[124](#) Distinguishing — classes

~~122~~[125](#) Regulations — codes of conduct and certification programs

~~123~~[126](#) Whistleblowing

~~124~~[127](#) Prohibition

~~125~~[128](#) Offence and punishment

~~126~~[129](#) Review by parliamentary committee

## **PART 3** **Coming into Force**

[130](#) Order in council

## **Consequential and Related Amendments**

- 3**     *Personal Information Protection and Electronic Documents Act*
- 9**     *Access to Information Act*
- 10**    *Aeronautics Act*
- 11**    *Canada Evidence Act*
- 13**    *Canadian Radio-television and Telecommunications Commission Act*
- 14**    *Competition Act*
- 15**    *Canada Business Corporations Act*
- 16**    [Telecommunications Act](#)
- 17**    *Public Servants Disclosure Protection Act*
- 1920** Chapter 23 of the Statutes of Canada, 2010
- 3132** *Transportation Modernization Act*

## **Terminology**

- 3233** Replacement of "*Personal Information Protection and Electronic Documents Act*"

## **Transitional Provisions**

- 3334** Definitions

## **Coordinating Amendments**

- 34**
- 35**    [Bill C-11](#)
- 36**    2018, c. 10

## **PART 2**

**Personal Information and Data Protection Tribunal [Act](#) [Enactment of Act](#)**

**3537** Enactment

**An Act to establish the Personal Information and Data Protection Tribunal**

- 1 *Personal Information and Data Protection Tribunal Act*
- 2 Definition of *Minister*
- 3 Order designating Minister
- 4 Establishment
- 5 Jurisdiction
- 6 Members
- 7 Chairperson and Vice-Chairperson
- 8 Duties of Chairperson
- 9 Acting Chairperson
- 10 Term of office
- 11 Remuneration
- 12 Inconsistent interests
- 13 Principal office
- 14 Sittings
- 15 Nature of hearings
- 16 Powers
- 17 Reasons
- 18 Public availability — decisions
- 19 Rules
- 20 ~~Costs~~Cost
- 21 Decisions final

**Related Amendment to the Administrative Tribunals Support Service of Canada Act**

**38**

**PART 3**  
**Artificial Intelligence and Data Act**

**39** Enactment of Act

**An Act respecting artificial intelligence systems and data used in artificial intelligence systems**

**Short Title**

1 *Artificial Intelligence and Data Act*

**Definitions and Application**

2 Definitions

3 Non-application

**Purposes of Act**

4 Purposes

**PART 1**  
**Regulation of Artificial Intelligence Systems in the Private Sector**

**Interpretation**

5 Definitions

**Requirements**

6 Anonymized data

7 Assessment — high-impact system

8 Measures related to risks

9 Monitoring of mitigation measures

10 Keeping general records

11 Publication of description — making system available for use

12 Notification of material harm

### **Ministerial Orders**

13 Provision of subsection 10(1) records

14 Provision of subsection 10(2) records

15 Audit

16 Implementation of measures

17 Cessation

18 Publication

19 Compliance

20 Filing — Federal Court

21 *Statutory Instruments Act*

### **Information**

22 Confidential nature maintained

23 Obligation of Minister

24 Disclosure of confidential business information — subpoena, warrant, etc.

25 Disclosure of information — analyst

26 Disclosure of information — others

27 Publication of information — contravention

28 Publication of information — harm

### **Administrative Monetary Penalties**

29 Administrative monetary penalties

## Offences

30 Contravention — sections 6 to 12

## Administration

31 Designation

32 General powers of Minister

33 Artificial Intelligence and Data Commissioner

34 Analysts

35 Advisory committee

36 Regulations — Governor in Council

37 Regulations — Minister

## PART 2

### General Offences Related to Artificial Intelligence Systems

38 Possession or use of personal information

39 Making system available for use

40 Punishment

## **PART 3**

### **Coming into Force**

**37**

41 Order in council

## PART 4

### Coming into Force

40 Order in council

**SCHEDULE**

**SCHEDULE**



~~2nd~~<sup>1st</sup> Session, ~~43rd~~<sup>44th</sup> Parliament,  
~~69~~<sup>70-71</sup> Elizabeth II, ~~2020~~<sup>2021-2022</sup>

HOUSE OF COMMONS OF CANADA

**BILL C-~~11~~<sup>27</sup>**

An Act to enact the Consumer Privacy Protection Act ~~and~~, 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

**Preamble**

Whereas there is a need to modernize Canada's legislative framework so that it is suited to the digital age;

Whereas the protection of the privacy interests of individuals with respect to their personal information is essential to individual autonomy and dignity and to the full enjoyment of fundamental rights and freedoms in Canada;

Whereas Parliament recognizes the importance of the privacy and data protection principles contained in various international instruments;

Whereas trust in the digital and data-driven economy is key to ensuring its growth and fostering a more inclusive and prosperous Canada;

Whereas Canada is a trading nation and trade and commerce rely on the analysis, circulation and exchange of personal information and data across borders and geographical boundaries;

Whereas the design, development and deployment of artificial intelligence systems across provincial and international borders should be consistent with national and international standards to protect individuals from potential harm;

Whereas organizations of all sizes operate in the digital and data-driven economy and an agile regulatory framework is necessary to facilitate compliance with rules by, and promote innovation within, those organizations;

Whereas individuals expect a regulatory framework that ensures transparency and accountability with respect to how organizations handle their personal information and that is backed by meaningful enforcement;

Whereas the modernization of national standards for privacy protection to align them with international standards ensures a level playing field for organizations across Canada and assists them in maintaining their competitive position;

Whereas a modern regulatory framework governing the protection of personal information should promote the responsible collection, use and disclosure of such information by organizations for purposes that are in the public interest;

Whereas Parliament recognizes that artificial intelligence systems and other emerging technologies should uphold Canadian norms and values in line with the principles of international human rights law;

And whereas this Act aims to support the Government of Canada's efforts to foster an environment in which Canadians can seize the benefits of the digital and data-driven economy and to establish a regulatory framework that supports and protects Canadian norms and values, including the right to privacy;

Now, therefore, Her Majesty, by and with the advice and consent of the Senate and House of Commons of Canada, enacts as follows:

Short Title

**Short title**

1 This Act may be cited as the *Digital Charter Implementation Act*, ~~2020~~2022.

**PART 1**

Consumer Privacy Protection Act

Enactment of Act

**Enactment**

**2 The *Consumer Privacy Protection Act*, whose text is as follows and whose schedule is set out in the schedule to this Act, is enacted:**

An Act to support and promote electronic commerce by protecting personal information that is collected, used or disclosed in the course of commercial activities

Short Title

**Short title**

1 This Act may be cited as the *Consumer Privacy Protection Act*.

Interpretation

## Definitions

~~2 The following definitions apply in this Act.~~ (1) The following definitions apply in this Act.

*alternative format*, with respect to personal information, means a format that allows an individual with a sensory disability to read or listen to the personal information.

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

*automated decision system* means any technology that assists or replaces the ~~judgement~~judgment of human decision-makers ~~using techniques such as~~through the use of a rules-based ~~systems~~system, regression analysis, predictive analytics, machine learning, deep learning ~~and, a~~ neural ~~nets~~network or other technique.

*breach of security safeguards* means the loss of, unauthorized access to or unauthorized disclosure of personal information resulting from a breach of an organization's security safeguards that are referred to in section ~~57~~ or from a failure to establish those safeguards.

*business transaction* includes

- (a) the purchase, sale or other acquisition or disposition of an organization or a part of an organization, or any of its assets;
- (b) the merger or amalgamation of two or more organizations;
- (c) the making of a loan or provision of other financing to an organization or a part of an organization;
- (d) the creating of a charge on, or the taking of a security interest in or a security on, any assets or securities of an organization;
- (e) the lease or licensing of any of an organization's assets; and
- (f) any other prescribed arrangement between two or more organizations to conduct a business activity.

*commercial activity* means any particular transaction, act or conduct or any regular course of conduct that is of a commercial character, ~~taking into account an organization's objectives for carrying out the transaction, act or conduct, the context in which it takes place, the persons involved and its outcome~~including the selling, bartering or leasing of donor, membership or other fundraising lists.

*Commissioner* means the Privacy Commissioner appointed under section 53 of the *Privacy Act*.

**de-identify** means to modify personal information ~~—or create information from personal information—~~ by using technical processes to ensure that the information does not identify so that an individual ~~or could not~~ cannot be ~~used in reasonably foreseeable circumstances, alone or in combination with other information, to identify an~~ directly identified from it, though a risk of the individual being identified remains.

**disposal** dispose means ~~the permanent and irreversible deletion of~~ to permanently and irreversibly delete personal information or to anonymize it.

**federal work, undertaking or business** means any work, undertaking or business that is within the legislative authority of Parliament. It includes

- (a) a work, undertaking or business that is operated or carried on for or in connection with navigation and shipping, whether inland or maritime, including the operation of ships and transportation by ship anywhere in Canada;
- (b) a railway, canal, telegraph or other work or undertaking that connects a province with another province, or that extends beyond the limits of a province;
- (c) a line of ships that connects a province with another province, or that extends beyond the limits of a province;
- (d) a ferry between a province and another province or between a province and a country other than Canada;
- (e) aerodromes, aircraft or a line of air transportation;
- (f) a radio broadcasting station;
- (g) a *bank* or an *authorized foreign bank* as defined in section 2 of the *Bank Act*;
- (h) a work that, although wholly situated within a province, is before or after its execution declared by Parliament to be for the general advantage of Canada or for the advantage of two or more provinces;
- (i) a work, undertaking or business outside the exclusive legislative authority of the legislatures of the provinces; and
- (j) a work, undertaking or business to which *federal laws*, within the meaning of section 2 of the *Oceans Act*, apply under section 20 of that Act and any regulations made under paragraph 26(1)(k) of that Act.

**Minister** means the member of the Queen's Privy Council for Canada designated under section 3 or, if no member is designated, the Minister of Industry.

**organization** includes an association, a partnership, a person or a trade union.

**personal information** means information about an identifiable individual.

*prescribed* means prescribed by regulation.

*record* means any documentary material, regardless of medium or form.

*service provider* means an organization, including a parent corporation, subsidiary, affiliate, contractor or subcontractor, that provides services for or on behalf of another organization to assist the organization in fulfilling its purposes.

*Tribunal* means the Personal Information and Data Protection Tribunal established under section 4 of the *Personal Information and Data Protection Tribunal Act*. ([Tribunal](#))

### Interpretation — minors

(2) For the purposes of this Act, the personal information of minors is considered to be sensitive information.

### Interpretation — de-identified information

(3) For the purposes of this Act, other than sections 20 and 21, subsections 22(1) and 39(1), sections 55 and 56, subsection 63(1) and sections 71, 72, 74, 75 and 116, personal information that has been de-identified is considered to be personal information.

### **Order designating Minister**

3 The Governor in Council may, by order, designate any member of the Queen's Privy Council for Canada to be the Minister for the purposes of this Act.

### **Authorized representatives**

4 The rights and recourses provided under this Act may be exercised

(a) on behalf of a minor ~~or an individual under any other legal incapacity by a person authorized by or under law to administer the affairs or property of that individual~~ by a parent, guardian or tutor, unless the minor wishes to personally exercise those rights and recourses and is capable of doing so;

(b) on behalf of ~~a deceased~~ an individual, other than a minor, under a legal incapacity by a person authorized by ~~or under~~ law to administer the ~~estate~~ affairs or ~~succession~~ property of that individual, ~~but only for the purpose of that administration;~~ and

(c) on behalf of ~~any other~~ a deceased individual by ~~any~~ a person authorized ~~in writing~~ by law to ~~do so by~~ administer the estate or succession of that individual, ~~but only for the purpose of that administration.~~

### Purpose and Application

#### **Purpose**

**5** The purpose of this Act is to establish — 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 — rules to govern the protection of personal information in a manner that recognizes the right of privacy of individuals with respect to their personal information and the need of organizations to collect, use or disclose personal information for purposes that a reasonable person would consider appropriate in the circumstances.

### **Application**

**6 (1)** This Act applies to every organization in respect of personal information that

- (a) the organization collects, uses or discloses in the course of commercial activities; or
- (b) is about an employee of, or an applicant for employment with, the organization and that the organization collects, uses or discloses in connection with the operation of a federal work, undertaking or business.

### **For greater certainty**

**(2)** For greater certainty, this Act applies in respect of personal information

- (a) that is collected, used or disclosed interprovincially or internationally by an organization; or
- (b) that is collected, used or disclosed by an organization within a province, to the extent that the organization is not exempt from the application of this Act under an order made under paragraph ~~119(2)~~[122\(2\)](#)(b).

### **Application**

**(3)** This Act also applies to an organization set out in column 1 of the schedule in respect of personal information set out in column 2.

### **Limit**

**(4)** This Act does not apply to

- (a) any government institution to which the *Privacy Act* applies;
- (b) any individual in respect of personal information that the individual collects, uses or discloses solely for personal or domestic purposes;
- (c) any organization in respect of personal information that the organization collects, uses or discloses solely for journalistic, artistic or literary purposes;
- (d) any organization in respect of an individual's personal information that the organization collects, uses or discloses solely for the purpose of communicating or facilitating communication with the individual in relation to their employment, business or profession; or

(e) any organization that is, under an order made under paragraph ~~119(2122(2))~~(b), exempt from the application of this Act in respect of the collection, use or disclosure of personal information that occurs within a province in respect of which the order was made.

### For greater certainty

(5) For greater certainty, this Act does not apply in respect of personal information that has been anonymized.

### **Other Acts**

~~(5)~~ Every provision of this Act applies despite any provision, enacted after December 31, 2000, of any other Act of Parliament, unless the other Act expressly declares that that provision operates despite the provision of this Act.

## **PART 1**

### **Obligations of Organizations**

#### Accountability of Organizations

#### **Accountability — personal information under organization's control**

7 (1) An organization is accountable for personal information that is under its control.

#### **Personal information under control of organization**

(2) Personal information is under the control of the organization that decides to collect it and that determines the purposes for its collection, use or disclosure, regardless of whether the information is collected, used or disclosed by the organization itself or by a service provider on behalf of the organization.

#### **Designated individual**

8 (1) An organization must designate one or more individuals to be responsible for matters related to its obligations under this Act. It must provide the designated individual's business contact information to any person who requests it.

#### **Effect of designation of individual**

(2) The designation of an individual under subsection (1) does not relieve the organization of its obligations under this Act.

#### **Privacy management program**

9 (1) Every organization must implement and maintain a privacy management program that includes the ~~organization's~~ policies, practices and procedures the organization has put in place to ~~fulfil~~fulfill its obligations under this Act, including policies, practices and procedures respecting

- (a) the protection of personal information;
- (b) how requests for information and complaints are received and dealt with;
- (c) the training and information provided to the organization's staff respecting its policies, practices and procedures; and
- (d) the development of materials to explain the organization's policies and procedures ~~put in place to fulfil its obligations under this Act.~~

### **Volume and sensitivity**

(2) In developing its privacy management program, the organization must take into account the volume and sensitivity of the personal information under its control.

Access ~~by Commissioner — policies, practices and procedures~~ privacy management program

10 (1) An organization must, on request of the Commissioner, provide the Commissioner with access to the policies, practices and procedures that are included in its privacy management program.

### **Guidance and corrective measures**

(2) The Commissioner may, after reviewing the policies, practices and procedures, provide guidance on, or recommend that corrective measures be taken by the organization in relation to, its privacy management program.

### **Same protection**

11 (1) If an organization transfers personal information to a service provider, the organization must ensure, by contract or otherwise, that the service provider provides ~~substantially the same~~ level of protection of the personal information ~~as~~ equivalent to that which the organization is required to provide under this Act.

### **Service provider obligations**

(2) The obligations under this Part, other than those set out in sections 57 and 61, do not apply to a service provider in respect of personal information that is transferred to it. However, the service provider is subject to all of the obligations under this Part if it collects, uses or discloses that information for any purpose other than the purposes for which the information was transferred.

Appropriate Purposes

### **Appropriate purposes**



**12 (1)** 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, whether or not consent is required under this Act.

### **Factors to consider**

(2) The following factors must be taken into account in determining whether the manner and purposes referred to in subsection (1) are appropriate:

- (a) the sensitivity of the personal information;
- (b) whether the purposes represent legitimate business needs of the organization;
- (c) the effectiveness of the collection, use or disclosure in meeting the organization's legitimate business needs;
- (d) whether there are less intrusive means of achieving those purposes at a comparable cost and with comparable benefits; and
- (e) whether the individual's loss of privacy is proportionate to the benefits in light of anythe measures, technical or otherwise, implemented by the organization to mitigate the impacts of the loss of privacy on the individual.

### **Purposes**

(3) An organization must determine at or before the time of the collection of any personal information each of the purposes for which the information is to be collected, used or disclosed and record those purposes.

### **New purpose**

(4) If the organization determines that the personal information it has collected is to be used or disclosed for a new purpose, the organization must record that new purpose before using or disclosing that information for the new purpose.

### **Limiting Collection, Use and Disclosure**

#### **Limiting collection**

**13** The organization may collect only the personal information that is necessary for the purposes determined and recorded under subsection 12(3).

#### **New purpose**

**14 (1)** An organization must not use or disclose personal information for a purpose other than a purpose determined and recorded under subsection 12(3), unless the organization obtains the individual's valid consent before any use or disclosure for that other purpose.

### **Use or disclosure — other purposes**

(2) Despite subsection (1), an organization may

(a) use personal information for a purpose other than a purpose determined and recorded under subsection 12(3) in any of the circumstances set out in sections 18, 20 and 21, subsections 22(1) and (23) and sections 23, 24, 26, 30, 41 and 51; or

(b) disclose personal information for a purpose other than a purpose determined and recorded under subsection 12(3) in any of the circumstances set out in subsections 22(1) and (23), sections 23 to 28, 31 to 37 and 39, subsection 40(3) and sections 42 and 43 to 51.

Consent

### **Consent required**

**15 (1)** Unless this Act provides otherwise, an organization must obtain an individual's valid consent for the collection, use or disclosure of the individual's personal information.

### **Timing of consent**

(2) The individual's consent must be obtained at or before the time of the collection of the personal information or, if the information is to be used or disclosed for a purpose other than a purpose determined and recorded under subsection 12(3), before any use or disclosure of the information for that other purpose.

### **Information for consent to be valid**

(3) The individual's consent is valid only if, at or before the time that the organization seeks the individual's consent, it provides the individual with the following information ~~in plain language~~:

- (a) the purposes for the collection, use or disclosure of the personal information determined by the organization and recorded under subsection 12(3) or (4);
- (b) the ~~way~~manner in which the personal information is to be collected, used or disclosed;
- (c) any reasonably foreseeable consequences of the collection, use or disclosure of the personal information;
- (d) the specific type of personal information that is to be collected, used or disclosed; and
- (e) the names of any third parties or types of third parties to which the organization may disclose the personal information.

### **Plain language**

(4) The organization must provide the information referred to in subsection (3) in plain language that an individual to whom the organization's activities are directed would reasonably be expected to understand.

## Form of consent

(45) Consent must be expressly obtained; ~~unless the organization establishes that, subject to subsection (6),~~ it is appropriate to rely on an individual's implied consent, taking into account the reasonable expectations of the individual and the sensitivity of the personal information that is to be collected, used or disclosed.

## Business activities

(6) It is not appropriate to rely on an individual's implied consent if their personal information is collected or used for an activity described in subsection 18(2) or (3).

## Consent — provision of product or service

(57) The organization must not, as a condition of the ~~supply~~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.

## Consent obtained by deception

16 An organization must not obtain or attempt to obtain an individual's consent by providing false or misleading information or using deceptive or misleading practices. Any consent obtained under those circumstances is invalid.

## Withdrawal of consent

17 (1) On giving reasonable notice to an organization, an individual may, at any time, subject to this Act, to federal or provincial law or to the reasonable terms of a contract, withdraw their consent in whole or in part.

## Collection, use or disclosure to cease

(2) On receiving the notice from the individual, the organization must inform the individual of the consequences of the withdrawal of their consent and, as soon as feasible after that, cease the collection, use or disclosure of the individual's personal information in respect of which the consent was withdrawn.

## Exceptions to Requirement for Consent

### Business Operations

## Business activities

18 (1) An organization may collect or use an individual's personal information without their knowledge or consent if the collection or use is made for the purpose of a business activity described in subsection (2) and

- (a) a reasonable person would expect ~~such a~~the collection or use for ~~that~~such an activity;
- and

(b) the personal information is not collected or used for the purpose of influencing the individual's behaviour or decisions.

### List of activities

(2) Subject to the regulations, the following activities are business activities for the purpose of subsection (1):

(a) an activity that is necessary to provide ~~or deliver~~ a product or service that the individual has requested from the organization;

~~(b) an activity that is carried out in the exercise of due diligence to prevent or reduce the organization's commercial risk;~~

~~(c)~~ an activity that is necessary for the organization's information, system or network security;

~~(d)~~ an activity that is necessary for the safety of a product or service that the organization provides ~~or delivers~~;

~~(e) an activity in the course of which obtaining the individual's consent would be impracticable because the organization does not have a direct relationship with the individual;~~ and

~~(f)~~ any other prescribed activity.

### Legitimate interest

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

(a) a reasonable person would expect the collection or use for such an activity; and

(b) the personal information is not collected or used for the purpose of influencing the individual's behaviour or decisions.

### Conditions precedent

(4) Prior to collecting or using personal information under subsection (3), the organization must

(a) identify any potential adverse effect on the individual that is likely to result from the collection or use;

(b) identify and take reasonable measures to reduce the likelihood that the effects will occur or to mitigate or eliminate them; and

(c) comply with any prescribed requirements.

### Record of assessment

(5) The organization must record its assessment of how it meets the conditions set out in subsection (4) and must, on request, provide a copy of the assessment to the Commissioner.

### **Transfer to service provider**

**19** An organization may transfer an individual's personal information to a service provider without their knowledge or consent.

### **De-identification of personal information**

**20** An organization may use an individual's personal information without their knowledge or consent to de-identify the information.

### **Research, analysis and development**

**21** An organization may 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.

### **Prospective business transaction**

**22 (1)** Organizations that are parties to a prospective business transaction may use and disclose an individual's personal information without their knowledge or consent if

- (a) the information is de-identified before it is used or disclosed and remains so until the transaction is completed;
- (b) the organizations have entered into an agreement that requires the organization that receives the information
  - (i) to use and disclose that information solely for purposes related to the transaction,
  - (ii) to protect the information by security safeguards ~~appropriate~~proportionate to the sensitivity of the information, and
  - (iii) if the transaction does not proceed, to return the information to the organization that disclosed it, or dispose of it, within a reasonable time;
- (c) the organizations comply with the terms of that agreement; and
- (d) the information is necessary
  - (i) to determine whether to proceed with the transaction, and
  - (ii) if the determination is made to proceed with the transaction, to complete it.

### Exception — paragraph (1)(a)

(2) The requirement referred to in paragraph (1)(a) does not apply if it 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 information.

### **Completed business transaction**

(23) If the business transaction is completed, the organizations that are parties to the transaction may use and disclose the personal information referred to in subsection (1) without the individual's knowledge or consent if

- (a) the organizations have entered into an agreement that requires each of them
  - (i) to use and disclose the information under its control solely for the purposes for which the information was collected or permitted to be used or disclosed before the transaction was completed,
  - (ii) to protect that information by security safeguards ~~appropriate~~proportionate to the sensitivity of the information, and
  - (iii) to give effect to any withdrawal of consent made under subsection 17(1);
- (b) the organizations comply with the terms of that agreement;
- (c) the information is necessary for carrying on the business or activity that was the object of the transaction; and
- (d) one of the parties notifies the individual, within a reasonable time after the transaction is completed, that the transaction has been completed and that their information has been disclosed under subsection (1).

### **Exception**

(34) Subsections (1) and (23) do not apply to a business transaction of which the primary purpose or result is the purchase, sale or other acquisition or disposition, or lease, of personal information.

### **Information produced in employment, business or profession**

23 An organization may collect, use or disclose an individual's personal information without their knowledge or consent if it was produced by the individual in the course of their employment, business or profession and the collection, use or disclosure is consistent with the purposes for which the information was produced.

### **Employment relationship — federal work, undertaking or business**

24 An organization that operates a federal, work, undertaking or business may collect, use or disclose an individual's personal information without their consent if

(a) the collection, use or disclosure is necessary to establish, manage or terminate an employment relationship between the organization and the individual in connection with the operation of a federal work, undertaking or business; and

(b) the organization has informed the individual that the personal information will be or may be collected, used or disclosed for those purposes.

### **Disclosure to lawyer or notary**

**25** An organization may disclose an individual's personal information without their knowledge or consent to a lawyer or, in Quebec, a lawyer or notary, who is representing the organization.

### **Witness statement**

**26** An organization may collect, use or disclose an individual's personal information without their knowledge or consent if the information is contained in a witness statement and the collection, use or disclosure is necessary to assess, process or settle an insurance claim.

### **Prevention, detection or suppression of fraud**

**27 (1)** An organization may disclose an individual's personal information to another organization without the individual's knowledge or consent if the disclosure is reasonable for the purposes of detecting or suppressing fraud or of preventing fraud that is likely to be committed and it is reasonable to expect that the disclosure with the individual's knowledge or consent would compromise the ability to prevent, detect or suppress the fraud.

### **Collection**

(2) An organization may collect or use an individual's personal information without their knowledge or consent if the information was disclosed to it under subsection (1).

### **Debt collection**

**28** An organization may disclose an individual's personal information without their knowledge or consent for the purpose of collecting a debt owed by the individual to the organization.

### **Public Interest**

### **Individual's interest**

**29 (1)** An organization may collect an individual's personal information without their knowledge or consent if the collection is clearly in the interests of the individual and consent cannot be obtained in a timely way.

### **Use**

(2) An organization may use an individual's personal information without their knowledge or consent if the information was collected under subsection (1).

### **Emergency — use**

**30** An organization may use an individual's personal information without their knowledge or consent for the purpose of acting in respect of an emergency that threatens the life, health or security of any individual.

### **Emergency — disclosure**

**31** An organization may disclose an individual's personal information without their knowledge or consent to a person who needs the information because of an emergency that threatens the life, health or security of any individual. If the individual whom the information is about is alive, the organization must inform that individual in writing without delay of the disclosure.

### **Identification of individual**

**32** An organization may disclose an individual's personal information without their knowledge or consent if the disclosure is necessary to identify the individual who is injured, ill or deceased and is made to a government institution, a part of a government institution or the individual's next of kin or authorized representative. If the individual is alive, the organization must inform them in writing without delay of the disclosure.

### **Communication with next of kin or authorized representative**

**33** An organization may disclose an individual's personal information without their knowledge or consent to a government institution or part of a government institution that has made a request for the information, identified its lawful authority to obtain the information and indicated that the disclosure is requested for the purpose of communicating with the next of kin or authorized representative of an injured, ill or deceased individual.

### **Financial abuse**

**34** An organization may on its own initiative disclose an individual's personal information without their knowledge or consent to a government institution, a part of a government institution or the individual's next of kin or authorized representative if

- (a) the organization has reasonable grounds to believe that the individual has been, is or may be the victim of financial abuse;
- (b) the disclosure is made solely for purposes related to preventing or investigating the abuse; and
- (c) it is reasonable to expect that disclosure with the knowledge or consent of the individual would compromise the ability to prevent or investigate the abuse.

### **~~Statistical or scholarly~~ Statistics, study or research**

**35** An organization may disclose an individual's personal information without their knowledge or consent if



- (a) the disclosure is made for statistical purposes or for ~~scholarly~~ study or research purposes and those purposes cannot be achieved without disclosing the information;
- (b) it is impracticable to obtain consent; and
- (c) the organization informs the Commissioner of the disclosure before the information is disclosed.

### **Records of historic or archival importance**

**36** An organization may disclose an individual's personal information without their knowledge or consent to an institution whose functions include the conservation of records of historic or archival importance, if the disclosure is made for the purpose of such conservation.

### **Disclosure after period of time**

**37** An organization may disclose an individual's personal information without their knowledge or consent after the earlier of

- (a) 100 years after the record containing the information was created, and
- (b) 20 years after the death of the individual.

### **Journalistic, artistic or literary purposes**

**38** An organization may collect an individual's personal information without their knowledge or consent if the collection is solely for journalistic, artistic or literary purposes.

### **Socially beneficial purposes**

**39 (1)** An organization may disclose an individual's personal information without their knowledge or consent if

- (a) the personal information is de-identified before the disclosure is made;
- (b) the disclosure is made to
  - (i) a government institution or part of a government institution in Canada,
  - (ii) a health care institution, post-secondary educational institution or public library in Canada,
  - (iii) any organization that is mandated, under a federal or provincial law or by contract with a government institution or part of a government institution in Canada, to carry out a socially beneficial purpose, or
  - (iv) any other prescribed entity; and
- (c) the disclosure is made for a socially beneficial purpose.

### **Definition of *socially beneficial purpose***

(2) For the purpose of this section, *socially beneficial purpose* means a purpose related to health, the provision or improvement of public amenities or infrastructure, the protection of the environment or any other prescribed purpose.

Investigations

### **Breach of agreement or contravention**

**40 (1)** An organization may collect an individual's personal information without their knowledge or consent if it is reasonable to expect that the collection with their knowledge or consent would compromise the availability or the accuracy of the information and the collection is reasonable for purposes related to investigating a breach of an agreement or a contravention of federal or provincial law.

Use

(2) An organization may use an individual's personal information without their knowledge or consent if the information was collected under subsection (1).

### **Disclosure**

(3) An organization may disclose an individual's personal information without their knowledge or consent if the disclosure is made to another organization and is reasonable for the purposes of investigating a breach of an agreement or a contravention of federal or provincial law that has been, is being or is about to be committed and it is reasonable to expect that disclosure with the knowledge or consent of the individual would compromise the investigation.

### **Use for investigations**

**41** An organization may use an individual's personal information without their knowledge or consent if, in the course of its activities, the organization becomes aware of information that it has reasonable grounds to believe could be useful in the investigation of a contravention of federal or provincial law or law of a foreign jurisdiction that has been, is being or is about to be committed and the information is used for the purpose of investigating that contravention.

### **Breach of security safeguards**

**42** An organization may disclose an individual's personal information without their knowledge or consent if

(a) the disclosure is made to the other organization, government institution or part of a government institution that was notified of a breach under subsection 59(1); and

(b) the disclosure is made solely for the purposes of reducing the risk of harm to the individual that could result from the breach or mitigating that harm.

## Disclosures to Government Institutions

### **Administering law — request of government institution**

**43** An organization may disclose an individual's personal information without their knowledge or consent to a government institution or part of a government institution that has made a request for the information, identified its lawful authority to obtain the information and indicated that the disclosure is requested for the purpose of administering federal or provincial law.

### **Law enforcement — request of government institution**

**44** An organization may disclose an individual's personal information without their knowledge or consent to a government institution or part of a government institution that has made a request for the information, identified its lawful authority to obtain the information and indicated that the disclosure is requested for the purpose of enforcing federal or provincial law or law of a foreign jurisdiction, carrying out an investigation relating to the enforcement of any such law or gathering intelligence for the purpose of enforcing any such law.

### **Contravention of law — initiative of organization**

**45** An organization may on its own initiative disclose an individual's personal information without their knowledge or consent to a government institution or a part of a government institution if the organization has reasonable grounds to believe that the information relates to a contravention of federal or provincial law or law of a foreign jurisdiction that has been, is being or is about to be committed.

### ***Proceeds of Crime (Money Laundering) and Terrorist Financing Act***

**46** An organization may disclose an individual's personal information without their knowledge or consent to the government institution referred to in section 7 of the *Proceeds of Crime (Money Laundering) and Terrorist Financing Act* as required by that section.

### **~~Request by government institution — national~~ National security, defence or international affairs — request by government institution**

**47 (1)** An organization may disclose an individual's personal information without their knowledge or consent to a government institution or part of a government institution that has made a request for the information, identified its lawful authority to obtain the information and indicated that it suspects that the information relates to national security, the defence of Canada or the conduct of international affairs.

### **Collection**

**(2)** An organization may collect an individual's personal information without their knowledge or consent for the purpose of making a disclosure under subsection (1).

### **Use**

(3) An organization may use an individual's personal information without their knowledge or consent if it was collected under subsection (2).

~~Initiative of organization — national~~ National security, defence or international affairs  
— initiative of organization

**48 (1)** An organization may on its own initiative disclose an individual's personal information without their knowledge or consent to a government institution or a part of a government institution if the organization suspects that the information relates to national security, the defence of Canada or the conduct of international affairs.

**Collection**

(2) An organization may collect an individual's personal information without their knowledge or consent for the purpose of making a disclosure under subsection (1).

**Use**

(3) An organization may use an individual's personal information without their knowledge or consent if it was collected under subsection (2).

Required by Law

**Required by law — collection**

**49 (1)** An organization may collect an individual's personal information without their knowledge or consent for the purpose of making a disclosure that is required by law.

**Use**

(2) An organization may use an individual's personal information without their knowledge or consent if it was collected under subsection (1).

**Disclosure**

(3) An organization may disclose an individual's personal information without their knowledge or consent if the disclosure is required by law.

**Subpoena, warrant or order**

**50** An organization may disclose an individual's personal information without their knowledge or consent if the disclosure is required to comply with a subpoena or warrant issued or an order made by a court, person or body with jurisdiction to compel the production of information, or to comply with rules of procedure relating to the production of records.

Publicly Available Information

**Information specified by regulations**

**51** An organization may collect, use or disclose an individual's personal information without their knowledge or consent if the personal information is publicly available and is specified by the regulations.

#### Non-application of Certain Exceptions — Electronic Addresses and Computer Systems

##### **Definitions**

**52 (1)** The following definitions apply in this section.

*access* means to program, execute programs on, communicate with, store data in, retrieve data from or otherwise make use of any resources, including data or programs of a computer system or a computer network.

*computer program* has the same meaning as in subsection 342.1(2) of the *Criminal Code*.

*computer system* has the same meaning as in subsection 342.1(2) of the *Criminal Code*.

*electronic address* means an address used in connection with

- (a) an electronic mail account;
- (b) an instant messaging account; or
- (c) any similar account.

##### **Collection and use of electronic addresses**

**(2)** An organization is not authorized under any of sections 18, 23 and 26, subsection 29(1) and sections 30, 38, 41 and 51 to

- (a) collect an individual's electronic address without their knowledge or consent, if the address is collected by the use of a computer program that is designed or marketed primarily for use in generating or searching for, and collecting, electronic addresses; or
- (b) use an individual's electronic address without their knowledge or consent, if the address is collected by the use of a computer program described in paragraph (a).

##### **Accessing computer system to collect personal information, etc.**

**(3)** An organization is not authorized under any of sections 18, 23 and 26, subsection 29(1), sections 30 and 38, subsection 40(1) and sections 41 and 51 to

- (a) collect an individual's personal information without their knowledge or consent, through any means of telecommunication, if the information is collected by accessing a computer system or causing a computer system to be accessed in contravention of an Act of Parliament; or

(b) use an individual's personal information without their knowledge or consent, if the information is collected in a manner described in paragraph (a).

### **Express consent**

(4) Despite subsection ~~15(4)~~[15\(5\)](#), an organization is not to rely on an individual's implied consent in respect of any collection of personal information described in paragraph (2)(a) or (3)(a) or any use of personal information described in paragraph (2)(b) or (3)(b).

### Retention and Disposal of Personal Information

#### **Period for retention and disposal**

**53 (1)** An organization must not retain personal information for a period longer than necessary to

- (a) ~~fulfill~~[fulfill](#) the purposes for which the information was collected, used or disclosed; or
- (b) comply with the requirements of this Act, of federal or provincial law or of the reasonable terms of a contract.

The organization must dispose of the information as soon as feasible after that period.

#### **Sensitivity of personal information**

(2) For the purposes of paragraph (1)(a), when determining the retention period, the organization must take into account the sensitivity of the information.

#### **Personal information used for decision-making**

**54** An organization that uses personal information to make a decision about an individual must retain the information for a sufficient period of time to permit the individual to make a request for access under section 63.

#### **Disposal at individual's request**

**55 (1)** If an organization receives a written request from an individual to dispose of their personal information that ~~it has collected from the individual~~[is under the organization's control](#), the organization must, as soon as feasible, dispose of the information, ~~unless~~[if](#)

(a) ~~disposing of~~ the information ~~would result in~~[was collected, used or disclosed in contravention of this Act;](#)

[\(b\) the individual has withdrawn their consent, in whole or in part, to the collection, use or disclosure of the information; or](#)

[\(c\) the information is no longer necessary for the continued provision of a product or service requested by the individual.](#)

## Exception

(2) An organization may refuse a request to dispose of personal information in the circumstances described in paragraph (1)(b) or (c) if

(a) disposing of the information would result in the disposal of personal information about another individual and the information is not severable;~~or~~

~~(b)~~(b) there are other requirements of this Act, of federal or provincial law or of the reasonable terms of a contract that prevent it from ~~doing so~~ disposing of the information;

(c) the information is necessary for the establishment of a legal defence or in the exercise of other legal remedies by the organization;

(d) the information is not in relation to a minor and the disposal of the information would have an undue adverse impact on the accuracy or integrity of information that is necessary to the ongoing provision of a product or service to the individual in question;

(e) the request is vexatious or made in bad faith; or

(f) the information is not in relation to a minor and it is scheduled to be disposed of in accordance with the organization's information retention policy, and the organization informs the individual of the remaining period of time for which the information will be retained.

## **Reasons for refusal**

~~(23)~~ An organization that refuses ~~a request to dispose of an individual's personal information~~ must inform ~~the individual~~ them in writing of the refusal, setting out the reasons and any recourse that they may have under section 73 or subsection 82(1).

## **Disposal of transferred personal information**

~~(34)~~ If an organization disposes of personal information at an individual's request, it must, as soon as feasible, inform any service provider to which it has transferred the information of the ~~individual's~~ request and ~~obtain a confirmation from~~ ensure that the service provider ~~that the information~~ has ~~been~~ disposed of the information.

## Accuracy of Personal Information

### **Accuracy of information**

**56 (1)** An organization must take reasonable steps to ensure that personal information under its control is as accurate, up-to-date and complete as is necessary to ~~fulfil~~ fulfill the purposes for which the information is collected, used or disclosed.

### **Extent of accuracy**

**(2)** In determining the extent to which personal information must be accurate, complete and up-to-date, the organization must take into account the individual's interests, including

- (a) whether the information may be used to make a decision about the individual;
- (b) whether the information is used on an ongoing basis; and
- (c) whether the information is disclosed to third parties.

### **Routine updating**

(3) An organization is not to routinely update personal information unless it is necessary to ~~fulfill~~fulfill the purposes for which the information is collected, used or disclosed.

### **Security Safeguards**

#### **Security safeguards**

57 (1) An organization must protect personal information through physical, organizational and technological security safeguards. The level of protection provided by those safeguards must be proportionate to the sensitivity of the information.

#### **Factors to consider**

(2) In addition to the sensitivity of the information, the organization must, in establishing its security safeguards, take into account the quantity, distribution, format and method of storage of the information.

#### **Scope of security safeguards**

(3) The security safeguards must protect personal information against, among other things, loss, theft and unauthorized access, disclosure, copying, use and modification and must include reasonable measures to authenticate the identity of the individual to whom the personal information relates.

#### **Report to Commissioner**

58 (1) An organization must report to the Commissioner any breach of security safeguards involving personal information under its control if it is reasonable in the circumstances to believe that the breach creates a real risk of significant harm to an individual.

#### **Report requirements**

(2) The report must contain the prescribed information and must be made in the prescribed form and manner as soon as feasible after the organization determines that the breach has occurred.

#### **Notification to individual**

(3) Unless otherwise prohibited by law, an organization must notify an individual of any breach of security safeguards involving the individual's personal information under the organization's control if it is reasonable in the circumstances to believe that the breach creates a real risk of significant harm to the individual.



### **Contents of notification**

(4) The notification must contain sufficient information to allow the individual to understand the significance to them of the breach and to take steps, if any are possible, to reduce the risk of harm that could result from it or to mitigate that harm. It must also contain any other prescribed information.

### **Form and manner**

(5) The notification must be conspicuous and must be given directly to the individual in the prescribed form and manner, except in prescribed circumstances, in which case it must be given indirectly in the prescribed form and manner.

### **Time to give notification**

(6) The notification must be given as soon as feasible after the organization determines that the breach has occurred.

### **Definition of *significant harm***

(7) For the purpose of this section, *significant harm* includes bodily harm, humiliation, damage to reputation or relationships, loss of employment, business or professional opportunities, financial loss, identity theft, negative effects on the credit record and damage to or loss of property.

### **Real risk of significant harm — factors**

(8) The factors that are relevant to determining whether a breach of security safeguards creates a real risk of significant harm to the individual include

- (a) the sensitivity of the personal information involved in the breach;
- (b) the probability that the personal information has been, is being or will be misused; and
- (c) any other prescribed factor.

### **Notification to organizations**

**59 (1)** An organization that notifies an individual of a breach of security safeguards under subsection 58(3) must notify any other organization, a government institution or a part of a government institution of the breach if the notifying organization believes that the other organization or the government institution or part concerned may be able to reduce the risk of harm that could result from it or mitigate that harm, or if any of the prescribed conditions are satisfied.

### **Time to give notification**

(2) The notification must be given as soon as feasible after the organization determines that the breach has occurred.

## Records

**60 (1)** An organization must, in accordance with any prescribed requirements, keep and maintain a record of every breach of security safeguards involving personal information under its control.

## Provision to Commissioner

(2) An organization must, on request, provide the Commissioner with access to, or a copy of, the record.

## Service providers

**61** 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.

## Openness and Transparency

## Policies and practices

**62 (1)** An organization must make readily available, in plain language, information that explains the organization's policies and practices put in place to ~~fulfil~~fulfill its obligations under this Act.

## Additional information

(2) In fulfilling its obligation under subsection (1), an organization must make the following information available:

- (a) a description of the type of personal information under the organization's control;
- (b) a general account of how the organization ~~makes use of~~uses the personal information, ~~including and of~~ how ~~the organization~~it applies the exceptions to the requirement to obtain an individual's consent under this Act, including a description of any activities referred to in subsection 18(3) in which it has a legitimate interest;
- (c) a general account of the organization's use of any automated decision system to make predictions, recommendations or decisions about individuals that could have a significant ~~impacts~~impact on them;
- (d) whether or not the organization carries out any international or interprovincial transfer or disclosure of personal information that may have reasonably foreseeable privacy implications;
- (e) the retention periods applicable to sensitive personal information;
- (f) how an individual may make a request for disposal under section 55 or access under section 63; and

(fg) the business contact information of the individual to whom complaints or requests for information may be made.

## Access to and Amendment of Personal Information

### Information and access

**63 (1)** On request by an individual, an organization must inform them of whether it has any personal information about them, how it uses the information and whether it has disclosed the information. It must also give the individual access to the information.

### Names or types of third parties

(2) If the organization has disclosed the information, the organization must also provide to the individual the names of the third parties or types of third parties to which the disclosure was made, including in cases where the disclosure was made without the consent of the individual.

### Automated decision system

(3) If the organization has used an automated decision system to make a prediction, recommendation or decision about the individual that could have a significant impact on them, the organization must, on request by the individual, provide them with an explanation of the prediction, recommendation or decision ~~and of how~~.

### Explanation

(4) The explanation must indicate the type of personal information that was used to make the prediction, recommendation or decision, the source of the information and the reasons or principal factors that led to the prediction, recommendation or decision ~~was obtained~~.

### Request in writing

**64 (1)** A request under section 63 must be made in writing.

### Assistance

(2) An organization must assist any individual who informs the organization that they need assistance in preparing a request to the organization.

### Information to be provided

**65** An organization may require the individual to provide it with sufficient information to allow the organization to ~~fulfil~~ fulfill its obligations under section 63.

### Plain language

**66 (1)** The information referred to in section 63 must be provided to the individual in plain language.

### **Sensory disability**

(2) For the purpose of section 63, an organization must give access to personal information in an alternative format to an individual with a sensory disability who requests that it be transmitted in that format if

- (a) a version of the information already exists in that format; or
- (b) its conversion into that format is reasonable and necessary in order for the individual to be able to exercise rights under this Act.

### **Sensitive medical information**

(3) An organization may choose to give an individual access to sensitive medical information through a medical practitioner.

### **Time limit**

**67 (1)** An organization must respond to a request made under section 63 with due diligence and in any case no later than 30 days after the day on which the request was received.

### **Extension of time limit**

(2) An organization may extend the time limit

- (a) for a maximum of 30 days if
  - (i) meeting the time limit would unreasonably interfere with the activities of the organization, or
  - (ii) the time required to undertake any consultations necessary to respond to the request would make the time limit impracticable to meet; or
- (b) for the period that is necessary in order to be able to convert the personal information into an alternative format.

In either case, the organization must, no later than 30 days after the day on which the request was received, send a notice of extension to the individual, advising them of the new time limit, the reasons for extending the time limit and their right to make a complaint to the Commissioner in respect of the extension.

### **Reasons**

(3) An organization that responds within the time limit and refuses a request must inform the individual in writing of the refusal, setting out the reasons and any recourse that they may have under section 73 or subsection 82(1).

### **Deemed refusal**

(4) If the organization fails to respond within the time limit, the organization is deemed to have refused the request.

### **Costs for responding**

**68** An organization must not respond to the individual's request made under section 63 at a cost unless

- (a) the organization has informed the individual of the approximate cost;
- (b) the cost to the individual is minimal; and
- (c) the individual has advised the organization that the request is not being withdrawn.

### **Retention of information**

**69** An organization that has personal information that is the subject of a request made under section 63 must retain the information for as long as is necessary to allow the individual to exhaust any recourse that they may have under this Act.

### **When access prohibited**

**70 (1)** Despite section 63, an organization must not give an individual access to personal information under that section if doing so would likely reveal personal information about another individual. However, if the information about the other individual is severable from the information about the requester, the organization must sever the information about the other individual before giving the requester access.

### **Limit**

(2) Subsection (1) does not apply if the other individual consents to the access or the requester needs the information because an individual's life, health or security is threatened.

### **Information related to certain exceptions to consent**

(3) An organization must comply with subsection (4) if an individual requests that the organization

- (a) inform the individual about
  - (i) any disclosure to a government institution or a part of a government institution under section 44, 45 or 46, subsection 47(1) or 48(1) or section 50, or
  - (ii) the existence of any information that the organization has relating to a disclosure referred to in subparagraph (i), to a subpoena, warrant or order referred to in section 50 or to a request made by a government institution or a part of a government institution under section 44 or subsection 47(1); or
- (b) give the individual access to the information referred to in subparagraph (a)(ii).

## Notification and response

(4) An organization to which subsection (3) applies

- (a) must, in writing and without delay, notify the institution or part concerned of the request made by the individual; and
- (b) must not respond to the request before the earlier of
  - (i) the day on which it is notified under subsection (5), and
  - (ii) 30 days after the day on which the institution or part is notified.

## Objection

(5) Within 30 days after the day on which it is notified under subsection (4), the institution or part must notify the organization of whether the institution or part objects to the organization complying with the request. The institution or part may object only if the institution or part is of the opinion that compliance with the request could reasonably be expected to be injurious to

- (a) national security, the defence of Canada or the conduct of international affairs;
- (b) the detection, prevention or deterrence of money laundering or the financing of terrorist activities; or
- (c) the enforcement of federal or provincial law or law of a foreign jurisdiction, an investigation relating to the enforcement of any such law or the gathering of intelligence for the purpose of enforcing any such law.

## Prohibition

(6) Despite section 63, if an organization is notified under subsection (5) that the institution or part objects to the organization complying with the request, the organization

- (a) must refuse the request to the extent that it relates to paragraph (3)(a) or to information referred to in subparagraph (3)(a)(ii);
- (b) must notify the Commissioner, in writing and without delay, of the refusal; ~~and~~
- (c) must not give the individual access to any information that the organization has relating to a disclosure to a government institution or a part of a government institution under section 44, 45 or 46, subsection 47(1) or 48(1) or section 50 or to a request made by a government institution or part of a government institution under section 44 or subsection 47(1); ~~and~~
- (d) must not provide to the individual the name of the government institution or part to which the disclosure was made or its type; and

(e) must not disclose to the individual the fact that the organization notified an institution or part under paragraph (4)(a), that the institution or part objects or that the Commissioner was notified under paragraph (b).

### **When access may be refused**

(7) Despite section 63, an organization is not required to give access to personal information if

(a) the information is protected by solicitor-client privilege or the professional secrecy of advocates and notaries or by litigation privilege;

(b) to do so would reveal confidential commercial information;

(c) to do so could reasonably be expected to threaten the life or security of another individual;

(d) the information was collected under subsection 40(1);

(e) the information was generated in the course of a formal dispute resolution process; or

(f) the information was created for the purpose of making a disclosure under the *Public Servants Disclosure Protection Act* or in the course of an investigation into a disclosure under that Act.

However, in the circumstances described in paragraph (b) or (c), if giving access to the information would reveal confidential commercial information or could reasonably be expected to threaten the life or security of another individual, as the case may be, and that information is severable from any other information for which access is requested, the organization must give the individual access after severing.

### **Limit**

(8) Subsection (7) does not apply if the individual needs the information because an individual's life, health or security is threatened.

### **Notice**

(9) If an organization decides not to give access to personal information in the circumstances set out in paragraph (7)(d), the organization must, in writing, notify the Commissioner, and must provide any information that the Commissioner may specify.

### **Amendment of personal information**

**71 (1)** 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.

### **Third party**

(2) The organization must, if it is appropriate to do so, transmit the amended information to any third party that has access to the information.

### **Record of determination**

(3) If the organization and the individual do not agree on the amendments that are to be made to the information, the organization must record the disagreement and, if it is appropriate to do so, inform third parties that have access to the information of the fact that there is a disagreement.

### Mobility of Personal Information

#### **Disclosure under data mobility framework**

72 Subject to the regulations, on the request of an individual, an organization must as soon as feasible disclose the personal information that it has collected from the individual to an organization designated by the individual, if both organizations are subject to a data mobility framework ~~provided under the regulations~~.

### Challenging Compliance

#### **Complaints and requests for information**

73 (1) An individual may make a complaint, or a request for information, to an organization with respect to its compliance with this Part. The organization must respond to any complaint or request that it receives.

#### **Process for making complaint or request**

(2) An organization must make readily available information about the process for making a complaint or request.

#### **Investigation of complaints**

(3) An organization must investigate any complaint that it receives and make any necessary changes to its policies, practices and procedures as a result of the investigation.

### De-identification of Personal Information

#### **Proportionality of technical and administrative measures**

74 An organization that de-identifies personal information must ensure that any technical and administrative measures applied to the information are proportionate to the purpose for which the information is de-identified and the sensitivity of the personal information.

#### **Prohibition**

75 An organization must not use information that has been de-identified ~~information~~, alone or in combination with other information, to identify an individual, ~~except in order~~



(a) to conduct testing of the effectiveness of security safeguards that ~~the organization~~it has put in place ;

(b) to ~~protect the information~~comply with any requirements under this Act or under federal or provincial law;

(c) to conduct testing of the fairness and accuracy of models, processes and systems that were developed using information that has been de-identified;

(d) to conduct testing of the effectiveness of its de-identification processes;

(e) for a purpose or situation authorized by the Commissioner under section 116; and

(f) in any other prescribed circumstance.

## **PART 2**

### **Commissioner's Powers, Duties and Functions and General Provisions**

Codes of Practice and Certification Programs

#### **Definition of *entity***

**76 (1)** For the purpose of this section and sections 77 to 81, *entity* includes any organization, regardless of whether it is an organization to which this Act applies, or a government institution.

#### **Code of practice**

(2) An entity may, in ~~the manner provided by~~accordance with the regulations, apply to the Commissioner 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 this Act.

#### **Approval by Commissioner**

(3) The Commissioner may approve the code of practice if the Commissioner determines that the code meets the criteria set out in the regulations.

#### **Certification program**

**77 (1)** An entity may, in ~~the manner provided by~~accordance with the regulations, apply to the Commissioner for approval of a certification program that includes

(a) 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 this Act;

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

- (c) a mechanism by which an entity that operates the program may certify that an organization is in compliance with the code of practice;
- (d) a mechanism for the independent verification of an organization's compliance with the code of practice;
- (e) disciplinary measures for non-compliance with the code of practice by an organization, including the revocation of an organization's certification; and
- (f) anything else that is provided in the regulations.

### **Approval by Commissioner**

(2) The Commissioner may approve the certification program if the Commissioner determines that the program meets the criteria set out in the regulations.

### **Response by Commissioner**

78 The Commissioner must respond in writing to an application under subsection 76(2) or 77(1) in the time specified in the regulations.

### **Approval made public**

79 The Commissioner must make public a decision to approve a code of practice or certification program.

### **For greater certainty**

80 For greater certainty, compliance with the requirements of a code of practice or a certification program does not relieve an organization of its obligations under this Act.

### **Powers of Commissioner**

81 The Commissioner may

- (a) request that an entity that operates an approved certification program provide the Commissioner with information that relates to the program;
- (b) cooperate with an entity that operates an approved certification program for the purpose of the exercise of the Commissioner's powers and the performance of the Commissioner's duties and functions under this Act;
- (c) in accordance with the regulations, recommend to an entity that operates an approved certification program that an organization's certification be withdrawn, in the circumstances and according to the criteria set out in the regulations, if the Commissioner is of the opinion that the organization is not in compliance with the requirements of the program;
- (d) disclose information to the Commissioner of Competition, under an agreement or arrangement entered into under section ~~445~~118, that relates to an entity that operates an

approved certification program or an organization that is certified under an approved certification program;

(e) in accordance with the regulations, revoke an approval of a certification program in the circumstances and according to the criteria set out in the regulations; or

(f) consult with federal government institutions respecting codes of practice or certification programs.

Recourses

Filing of Complaints

### **Contravention**

**82 (1)** An individual may file with the Commissioner a written complaint against an organization for contravening Part 1.

### **Commissioner may initiate complaint**

(2) If the Commissioner is satisfied that there are reasonable grounds to investigate a matter under this Act, the Commissioner may initiate a complaint in respect of the matter.

### **Time limit**

(3) A complaint that results from the refusal to grant a request made under section 63 must be filed within six months, or any longer period that the Commissioner allows, after the refusal or after the expiry of the time limit for responding to the request, as the case may be.

### **Notice**

(4) The Commissioner must give notice of a complaint to the organization against which the complaint was made, unless the Commissioner decides under ~~subsection 83(2)~~[section 84](#) not to carry out an investigation.

Investigation of Complaints and Dispute Resolution

### **Investigation of complaint by Commissioner**

**83 (1)** The Commissioner must carry out an investigation in respect of a complaint, unless the Commissioner is of the opinion that

(a) the complainant should first exhaust grievance or review procedures otherwise reasonably available;

(b) the complaint could more appropriately be dealt with, initially or completely, by means of a procedure provided for under any federal law, other than this Act, or provincial law;

(c) the complaint was not filed within a reasonable period after the day on which the subject matter of the complaint arose;~~or~~

(d) the complaint raises an issue in respect of which a certification program that was approved by the Commissioner under subsection 77(2) applies and the organization is certified under that program~~;~~

### **Exception**

~~(2) Despite subsection (1), the Commissioner is not required to carry out an investigation in respect of an act alleged 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.~~

### **Notification**

~~(3) The Commissioner must notify the complainant and the organization that the Commissioner will not investigate the complaint or any act alleged in the complaint and give reasons. However, if the decision is made for any of the reasons set out in subsection (2), the Commissioner must notify the complainant only.~~

### **Compelling reasons**

~~(4) The Commissioner may reconsider a decision not to investigate under subsection (1) if the Commissioner is satisfied that the complainant has established that there are compelling reasons to investigate.~~

### **Dispute resolution mechanisms**

~~84 The Commissioner may attempt to resolve a complaint by means of a dispute resolution mechanism such as mediation and conciliation, unless an inquiry is being conducted in respect of the complaint.~~

### **Discontinuance of Investigation**

#### **Reasons**

~~85 (1) The Commissioner may discontinue the investigation of a complaint if the Commissioner is of the opinion that~~

~~(a)~~

(e) there is insufficient evidence to pursue the investigation;

- (bf) the complaint is trivial, frivolous or vexatious or is made in bad faith;
- (eg) the organization has provided a fair and reasonable response to the complaint;
- (dh) the matter is already the object of an ongoing investigation or inquiry under this Act;
- (ei) the matter has already been the subject of a report or decision by the Commissioner;

~~(f) any of the circumstances referred to in paragraphs 83(1)(a) to (d) apply;~~

~~(gi) the matter is being or has already been addressed under a procedure referred to in paragraph 83(1)(a) or (b); or~~

~~(hk) the matter is the object of a compliance agreement entered into under subsection 86(187(1); or~~

(l) an investigation or any further investigation is unnecessary having regard to all the circumstances of the complaint.

#### ~~Other reason~~

#### Notification

(2) The Commissioner ~~may discontinue~~ 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. However, if the decision is made for any of the reasons set out in section 84, the Commissioner must not notify the organization.

#### Compelling reasons

(3) The Commissioner may reconsider a decision not to investigate under subsection (1) if the Commissioner is satisfied that the complainant has established that there are compelling reasons to investigate.

#### Exception

84 Despite subsection 83(1), the Commissioner is not required to carry out an investigation in respect of an act ~~alleged~~ 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.

## Discontinuance

85 The Commissioner may discontinue the investigation of a complaint if the Commissioner has formed an opinion referred to in subsection 83(1) or section 84. The Commissioner must notify the complainant and the organization of the discontinuance and give reasons for the decision.

## Dispute resolution mechanisms

86 The Commissioner may attempt to resolve a complaint by means of a dispute resolution mechanism such as mediation and conciliation, unless an inquiry is being conducted in respect of the complaint.

Compliance Agreements

### **Entering into compliance agreement**

**8687** (1) If, in the course of an investigation, 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, the Commissioner may enter into a compliance agreement with that organization, aimed at ensuring compliance with this Act.

### **Terms**

(2) A compliance agreement may contain any terms that the Commissioner considers necessary to ensure compliance with this Act.

### **Effect of compliance agreement**

(3) The Commissioner must not commence an inquiry under section ~~8889~~ in respect of any matter covered under the agreement.

### **For greater certainty**

(4) For greater certainty, a compliance agreement does not preclude the prosecution of an offence under this Act.

Notification

### **Notification and reasons**

**8788** The Commissioner must notify the complainant and the organization and give reasons for the decision if an investigation has ~~been discontinued or an investigation has~~ concluded and the Commissioner ~~will~~ has decided not ~~be conducting to conduct~~ an inquiry.

Inquiry

### **Inquiry — complaint**

**8889** (1) After investigating a complaint, the Commissioner may conduct an inquiry in respect of the complaint if the matter is not

- (a) the subject of dispute resolution under section **8486**;
- (b) discontinued; or
- (c) resolved.

#### **Notice**

(2) The Commissioner must give notice of the inquiry to the complainant and the organization.

#### **Inquiry — compliance agreement**

**8990** (1) If the Commissioner believes on reasonable grounds that an organization is not complying with the terms of a compliance agreement entered into under subsection **86(187(1))**, the Commissioner may conduct an inquiry in respect of the non-compliance.

#### **Notice**

(2) The Commissioner must give notice of the inquiry to the organization.

#### **Nature of inquiries**

**9091** (1) Subject to subsection (2), the Commissioner is not bound by any legal or technical rules of evidence in conducting an inquiry and must deal with the matter as informally and expeditiously as the circumstances and considerations of fairness and natural justice permit.

#### **Restriction**

(2) The Commissioner must not receive or accept as evidence anything that would be inadmissible in a court by reason of any privilege under the law of evidence.

#### **Opportunity to be heard**

(3) In conducting the inquiry, the Commissioner must give the organization and the complainant an opportunity to be heard and to be assisted or represented by counsel or by any person.

#### **Inquiry in private**

(4) The Commissioner may hold all or any part of the inquiry in private.

#### **Procedure**

**91**

#### **Rules**

92 The Commissioner ~~may determine~~ must make rules respecting the conduct of an inquiry, including the procedure and rules of evidence to be followed ~~in the conduct of an inquiry,~~ and must make ~~that procedure~~ those rules publicly available.

### **Decision**

9293 (1) The Commissioner must complete an inquiry by rendering a decision that sets out

- (a) the Commissioner's findings on whether the organization has contravened this Act or has not complied with the terms of a compliance agreement;
- (b) any order made under subsection (2);
- (c) any decision made under subsection ~~93(1)~~ 94(1); and
- (d) the Commissioner's reasons for the findings, order or decision.

### **Compliance order**

(2) The Commissioner may, to the extent that is reasonably necessary to ensure compliance with this Act, order the organization to

- (a) take measures to comply with this Act;
- (b) stop doing something that is in contravention of this Act;
- (c) comply with the terms of a compliance agreement that has been entered into by the organization; or
- (d) make public any measures taken or proposed to be taken to correct the policies, practices or procedures that the organization has put in place to ~~fulfil~~ fulfill its obligations under this Act.

### **Communication of decision**

(3) The decision must be sent to the complainant and the organization without delay.

### **Extension of time**

(4) An inquiry conducted under section ~~88~~ 89 must be completed within one year after the day on which the complaint is filed or is initiated by the Commissioner. However, the Commissioner may extend the time limit, for a period not exceeding one year, by notifying the complainant and the organization of the anticipated date on which the decision is to be made.

Administrative Monetary Penalties

### **Recommendation**



**9394** (1) If, ~~in~~on completing an inquiry under section ~~8889~~ or ~~8990~~, the Commissioner finds that an organization has contravened one or more of the following provisions, the Commissioner must decide whether to recommend that a penalty be imposed on the organization by the Tribunal:

(a) subsection 9(1);

(b) subsection 11(1);

(c) subsections 12(3) and (4);

(d) section 13;

(~~be~~) subsection 14(1);

(~~e~~) ~~subsection 15(5);~~ f) subsections 15(1) and (7);

(~~dg~~) section 16;

(~~eh~~) subsection 17(2);

(i) section 53;

(~~fi~~) subsections 55(1) and (3);

(~~gk~~) subsection 57(1); ~~and~~

(~~hl~~) subsections 58(1) and (3);

(m) section 61; and

(n) subsection 62(1).

### **Factors to consider**

(2) In making the decision, the Commissioner must take into account the following factors ~~into account~~:

(a) the nature and scope of the contravention;

(b) ~~whether~~ any evidence that the organization ~~has voluntarily paid compensation to a person affected by~~ exercised due diligence to avoid the contravention;

(c) whether the organization made reasonable efforts to mitigate or reverse the contravention's effects;

(d) the organization's history of compliance with this Act;

(e) any prescribed factor; and

~~(d)~~(f) any other relevant factor.

### **Limitation**

(3) The Commissioner must not recommend that a penalty be imposed on an organization if the Commissioner is of the opinion that, at the time of the contravention of the provision in question, the organization was in compliance with the requirements of a certification program that was in relation to that provision and was approved by the Commissioner under subsection 77(2).

### **Notice to Tribunal**

(4) If the Commissioner decides to recommend that a penalty be imposed on an organization, the Commissioner must file with the Tribunal a copy of the decision rendered under subsection ~~92(1)~~93(1) that sets out the decision to recommend.

### **Imposition of penalty**

~~94~~95 (1) The Tribunal may, by order, impose a penalty on an organization if

(a) the Commissioner files a copy of a decision in relation to the organization in accordance with subsection ~~93(4)~~94(4) or the Tribunal, on appeal, substitutes its own decision to recommend that a penalty be imposed on the organization for the Commissioner's decision not to recommend;

(b) the organization and the Commissioner are given the opportunity to make representations; and

(c) the Tribunal determines that imposing the penalty is appropriate.

### **Findings**

(2) In determining whether it is appropriate to impose a penalty on an organization, the Tribunal must rely on the findings set out in the decision that is rendered by the Commissioner under subsection ~~92(1)~~93(1) in relation to the organization or on the Tribunal's own findings if, on appeal, it substitutes its own findings for those of the Commissioner.

### **Limitations**

(3) The Tribunal must not impose a penalty on an organization in relation to a contravention if a prosecution for the act or omission that constitutes the contravention has been instituted against the organization or if the organization establishes that it exercised due diligence to prevent the contravention.

### **Maximum penalty**

(4) The maximum penalty for all the contraventions in a recommendation taken together is the higher of \$10,000,000 and 3% of the organization's gross global revenue in its financial year before the one in which the penalty is imposed.

### **Factors to consider**

(5) In determining whether it is appropriate to impose a penalty on an organization and in determining the amount of a penalty, the Tribunal must take the following factors into account:

- (a) the factors set out in subsection ~~93(2)~~[94\(2\)](#);
- (b) the organization's ability to pay the penalty and the likely effect of paying it on the organization's ability to carry on its business; and
- (c) any financial benefit that the organization obtained from the contravention.

### **Purpose of penalty**

(6) The purpose of a penalty is to promote compliance with this Act and not to punish.

### **Recovery as debt due to Her Majesty**

~~9596~~ A penalty imposed under section ~~94~~[95](#) constitutes a debt due to Her Majesty and the debt is payable and may be recovered by the Minister as of the day on which it is imposed.

Audits

### **Ensure compliance**

~~9697~~ The Commissioner may, on reasonable notice and at any reasonable time, audit the personal information management practices of an organization if the Commissioner has reasonable grounds to believe that the organization has contravened, is contravening or is likely to contravene Part 1.

### **Report of findings and recommendations**

~~9798~~ (1) After an audit, the Commissioner must provide the audited organization with a report that contains the findings of the audit and any recommendations that the Commissioner considers appropriate.

### **Reports may be included in annual reports**

(2) The report may be included in a report made under section ~~118~~[121](#).

Commissioner's Powers — Investigations, Inquiries and Audits

### **Powers of Commissioner**

~~9899~~ (1) In carrying out an investigation of a complaint, conducting an inquiry or carrying out an audit, the Commissioner may

- (a) summon and enforce the appearance of persons before the Commissioner and compel them to give oral or written evidence on oath and to produce any records and things that the Commissioner considers necessary to carry out the investigation, conduct the inquiry or carry out the audit, in the same manner and to the same extent as a superior court of record;
- (b) administer oaths;
- (c) receive and accept any evidence and other information, whether on oath, by affidavit or otherwise, that the Commissioner sees fit, whether or not it is or would be admissible in a court of law;
- (d) make any interim order that the Commissioner considers appropriate;
- (e) order an organization that has information that is relevant to the investigation, inquiry or audit to retain the information for as long as is necessary to allow the Commissioner to carry out the investigation, conduct the inquiry or carry out the audit;
- (f) at any reasonable time, enter any premises, other than a dwelling-house, occupied by an organization on satisfying any security requirements of the organization relating to the premises;
- (g) converse in private with any person in any premises entered under paragraph (f) and otherwise make any inquiries in those premises that the Commissioner sees fit; and
- (h) examine or obtain copies of or extracts from records found in any premises entered under paragraph (f) that contain any matter relevant to the investigation, inquiry or audit.

### **Return of records**

(2) The Commissioner or the Commissioner's delegate must return to a person or an organization any record or thing that they produced under this section within 10 days after the day on which they make a request to the Commissioner or the delegate, but nothing precludes the Commissioner or the delegate from again requiring that the record or thing be produced.

### **Delegation**

**99100** (1) The Commissioner may delegate any of the powers, duties or functions set out in sections 83 to ~~9697~~ and subsection ~~98(199(1))~~.

### **Certificate of delegation**

(2) Any person to whom powers set out in subsection ~~98(199(1))~~ are delegated must be given a certificate of the delegation and the delegate must produce the certificate, on request, to the person in charge of any premises to be entered under paragraph (f) of that subsection.

Appeals

### **Right of appeal**

**100101** (1) A complainant or organization that is affected by any of the following findings, orders or decisions may appeal it to the Tribunal:

- (a) a finding that is set out in a decision rendered under subsection ~~92(193(1))~~;
- (b) an order made under subsection ~~92(293(2))~~; or
- (c) a decision made under subsection ~~93(194(1))~~ not to recommend that a penalty be imposed on the organization.

#### **Time limit — appeal**

(2) The time limit for making an appeal is 30 days after the day on which the Commissioner renders the decision under subsection ~~92(193(1))~~ that sets out the finding, order or decision.

#### **Appeal with leave**

**101102** (1) A complainant or organization that is affected by an interim order made under paragraph ~~98(199(1))~~(d) may, with leave of the Tribunal, appeal the order to the Tribunal.

#### **Time limit — leave to appeal**

(2) The time limit for making an application for leave to appeal is 30 days after the day on which the order is made.

#### **Disposition of appeals**

**102103** (1) The Tribunal may dispose of an appeal by dismissing it or by allowing it and, in allowing the appeal, the Tribunal may substitute its own finding, order or decision for the one under appeal.

#### **Standard of review**

(2) The standard of review for an appeal is correctness for questions of law and palpable and overriding error for questions of fact or questions of mixed law and fact.

#### **Enforcement of Orders**

#### **Compliance orders**

**103104** (1) If an order made by the Commissioner under subsection ~~92(293(2))~~ is not appealed to the Tribunal or an appeal of the order is dismissed by the Tribunal, the order may, for the purposes of its enforcement, be made an order of the Federal Court and is enforceable in the same manner as an order of that Court.

#### **Interim orders**

(2) If an application for leave to appeal to the Tribunal is not made in relation to an order made by the Commissioner under paragraph ~~98(199(1))~~(d), a leave application in relation to the order is

dismissed by the Tribunal or a leave application in relation to the order is granted by the Tribunal but the appeal is dismissed, then the order may, for the purposes of its enforcement, be made an order of the Federal Court and is enforceable in the same manner as an order of that Court.

### **Tribunal orders**

**104105** If the Tribunal, on appeal, substitutes its own order for an order of the Commissioner made under subsection ~~92(293(2))~~ or paragraph ~~98(499(1))~~(d), the Tribunal's order may, for the purposes of its enforcement, be made an order of the Federal Court and is enforceable in the same manner as an order of that Court.

### **Filing with Court**

**105106** An order referred to in section ~~103104~~ or ~~104105~~ is made an order of the Federal Court by filing a certified copy of it with the Registrar of that Court.

### **Private Right of Action**

#### **Damages — contravention of Act**

**106107 (1)** An individual who is affected by an act or omission by an organization that constitutes a contravention of this Act has a cause of action against the organization for damages for loss or injury that the individual has suffered as a result of the contravention if

(a) the Commissioner has made a finding under paragraph ~~92(493(1))~~(a) that the organization has contravened this Act and

(i) the finding is not appealed and the time limit for making an appeal under subsection ~~100(2101(2))~~ has expired, or

(ii) the Tribunal has dismissed an appeal of the finding under subsection ~~102(4103(1))~~; or

(b) the Tribunal has made a finding under subsection ~~102(4103(1))~~ that the organization has contravened this Act.

#### **Damages — offence**

(2) If an organization has been convicted of an offence under section ~~125128~~, an individual affected by the act or omission that gave rise to the offence has a cause of action against the organization for damages for loss or injury that the individual has suffered as a result of the act or omission.

#### **Limitation period or prescription**

(3) An action must not be brought later than two years after the day on which the individual becomes aware of

(a) in the case of an action under subsection (1), the Commissioner's finding or, if there is an appeal, the Tribunal's decision; and

(b) in the case of an action under subsection (2), the conviction.

### **Court of competent jurisdiction**

(4) An action referred to in subsection (1) or (2) may be brought in the Federal Court or a superior court of a province.

Certificate Under Canada Evidence Act

### **Certificate under *Canada Evidence Act***

**107108** (1) If a certificate under section 38.13 of the *Canada Evidence Act* prohibiting the disclosure of personal information of a specific individual is issued before a complaint is filed by that individual under this Act in respect of a request for access to that information, the provisions of this Act respecting that individual's right of access to their personal information do not apply to the information that is subject to the certificate.

### **Certificate following filing of complaint**

(2) Despite any other provision of this Act, if a certificate under section 38.13 of the *Canada Evidence Act* prohibiting the disclosure of personal information of a specific individual is issued after the filing of a complaint under this Act in relation to a request for access to that information,

- (a) all proceedings under this Act in respect of that information, including an investigation, inquiry, audit, appeal or judicial review, are discontinued;
- (b) the Commissioner must not disclose the information and must take all necessary precautions to prevent its disclosure; and
- (c) the Commissioner must, within 10 days after the day on which the certificate is published in the *Canada Gazette*, return the information to the organization that provided the information.

### **Information not to be disclosed**

(3) The Commissioner and every person acting on behalf or under the direction of the Commissioner, in exercising their powers and performing their duties and functions under this Act, must not disclose information subject to a certificate issued under section 38.13 of the *Canada Evidence Act* and must take every reasonable precaution to avoid the disclosure of that information.

### **Power to delegate**

(4) The Commissioner must not delegate the investigation or inquiry in respect of any complaint relating to information subject to a certificate issued under section 38.13 of the *Canada Evidence Act* except to one of a maximum of four officers or employees of the Commissioner specifically designated by the Commissioner for the purpose of conducting that investigation or inquiry, as the case may be.

## Powers, Duties and Functions of Commissioner

### Factors to consider

~~108109~~ In addition to taking into account the purpose of this Act in the exercise of the Commissioner's exercising any powers and performing the ~~performance of the Commissioner's~~ any duties and functions under this Act, the Commissioner must take into account

(a) the purpose of this Act;

(b) the size and revenue of organizations;

(c) the volume and sensitivity of the personal information under their control; and

(d) matters of general public interest.

### Promoting purposes of Act

~~109110~~ (1) The Commissioner must, in the form and manner that the Commissioner considers appropriate,

(a) develop and conduct information programs to foster public understanding of this Act and recognition of its purposes;

(b) develop guidance materials and tools for organizations in relation to their compliance with this Act — including any guidance materials and tools that are requested by the Minister — in consultation with ~~affected~~ stakeholders, including any relevant federal government institutions;

(c) undertake and publish research that is related to the protection of personal information, including any research that is requested by the Minister;

(d) undertake and publish any research related to the operation or implementation of this Act that is requested by the Minister;

(e) on request by an organization, provide guidance on — and, if the organization's Commissioner considers it appropriate, recommend corrective measures in relation to — its privacy management program; and

(f) promote, by any other means that the Commissioner considers appropriate, the purposes of this Act.

### For greater certainty

(2) For greater certainty, for the purpose of paragraph (1)(e), the Commissioner may prioritize the requests of organizations that the Commissioner considers to be in greatest need of guidance and is not required to act on a request that the Commissioner considers unreasonable.

### Prohibition — use for initiating complaint or audit



**110111** The Commissioner must not use the information ~~they receive~~the Commissioner receives under section 10 or paragraph ~~109~~110(1)(e) as grounds to initiate a complaint under subsection 82(2) or to carry out an audit under section ~~96~~97 unless the Commissioner considers that the organization has wilfully disregarded the corrective measures that were recommended in relation to its privacy management program.

### **Information — powers, duties or functions**

**11112** The Commissioner must make readily available information on the manner in which the Commissioner exercises the Commissioner's powers or performs the Commissioner's duties or functions under this Act.

### **Confidentiality**

**112113** (1) Subject to subsections (3) to (8), section 79, paragraph 81(c), subsections 82(4) and ~~83(383(2))~~, section ~~87~~88, subsections ~~88(2) and~~ 89(2) and 90(2), section ~~92~~93, subsections ~~93(494(4))~~, ~~97(198(1))~~, ~~115(2118(2))~~, ~~116(3119(3))~~ and ~~117(1120(1))~~ and section ~~118~~121, the Commissioner or any person acting on behalf or under the direction of the Commissioner must not disclose any information that comes to their knowledge as a result of the exercise of any of the Commissioner's powers or the performance of any of the Commissioner's duties or functions under this Act other than those referred to in subsection 58(1) or 60(2).

### **Confidentiality — reports and records**

(2) Subject to subsections (3) to (8), section 79, paragraph 81(c), subsections 82(4) and ~~83(383(2))~~, section ~~87~~88, subsections ~~88(2) and~~ 89(2) and 90(2), section ~~92~~93, subsections ~~93(494(4))~~, ~~97(198(1))~~, ~~115(2118(2))~~, ~~116(3119(3))~~ and ~~117(1120(1))~~ and section ~~118~~121, the Commissioner or any person acting on behalf or under the direction of the Commissioner must not disclose any information contained in a report made under subsection 58(1) or in a record obtained under subsection 60(2).

### **Public interest**

(3) The Commissioner may, if the Commissioner considers that it is in the public interest to do so, make public any information that comes to the Commissioner's knowledge in the exercise of any of the Commissioner's powers or the performance of any of the Commissioner's duties or functions under this Act.

### **Disclosure of necessary information**

(4) The Commissioner may disclose, or may authorize any person acting on behalf or under the direction of the Commissioner to disclose, information that in the Commissioner's opinion is necessary to

- (a) carry out an investigation, conduct an inquiry or carry out an audit under this Act; or
- (b) establish the grounds for findings and recommendations contained in any decision or report made under this Act.

### **Disclosure in the course of proceedings**

(5) The Commissioner may disclose, or may authorize any person acting on behalf or under the direction of the Commissioner to disclose, information in the course of

- (a) a prosecution for an offence under section ~~125~~128;
- (b) a prosecution for an offence under section 132 of the *Criminal Code* (perjury) in respect of a statement made under this Act;
- (c) a proceeding or an appeal before the Tribunal under this Act; or
- (d) a judicial review in relation to the exercise of any of the Commissioner's powers or the performance of any of the Commissioner's duties or functions under this Act or in relation to a decision of the Tribunal.

### **Disclosure of offence authorized**

(6) The Commissioner may 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 the Commissioner's opinion, there is evidence of an offence.

### **Disclosure of breach of security safeguards**

(7) The Commissioner may disclose, or may authorize any person acting on behalf or under the direction of the Commissioner to disclose, to a government institution or a part of a government institution, any information contained in a report made under subsection 58(1) or in a record obtained under subsection 60(2) if the Commissioner has 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.

### **Disclosure**

(8) The Commissioner may disclose information, or may authorize any person acting on behalf or under the direction of the Commissioner to disclose information, in the course of proceedings in which the Commissioner has intervened under paragraph 50(c) 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 in accordance with subsection 58(3) or 60(1) of that Act.

### **Not competent witness**

~~113~~114 The Commissioner or any person acting on behalf or under the direction of the Commissioner is not a competent witness in respect of any matter that comes to their knowledge as

a result of the exercise of any of the Commissioner's powers or the performance of any of the Commissioner's duties or functions under this Act in any proceeding other than

- (a) a prosecution for an offence under section ~~125~~128;
- (b) a prosecution for an offence under section 132 of the *Criminal Code* (perjury) in respect of a statement made under this Act; or
- (c) a proceeding or an appeal before the Tribunal under this Act.

### **Protection of Commissioner**

~~114~~115 (1) No criminal or civil proceedings lie against the Commissioner, or against any person acting on behalf or under the direction of the Commissioner, for anything done, reported, decided or said in good faith as a result of the exercise or purported exercise of any power of the Commissioner or the performance or purported performance of any duty or function of the Commissioner under this Act.

### **Defamation**

(2) No action lies in defamation with respect to

- (a) anything said, any information supplied or any record or thing produced in good faith in the course of an investigation or audit carried out or an inquiry conducted by or on behalf of the Commissioner under this Act; and
- (b) any report or decision made in good faith by the Commissioner under this Act and any fair and accurate account of the report or decision made in good faith for the purpose of news reporting.

### **De-identified information**

116 For the purpose of paragraph 75(e), the Commissioner may, on request by an organization, authorize a purpose or situation in which the organization may use information that has been de-identified, alone or in combination with other information, to identify an individual if, in the Commissioner's opinion, it is clearly in the interests of the individual.

### **Agreements or arrangements — Minister**

117 The Commissioner may enter into an agreement or arrangement with the Minister relating to the administration of this Act.

### **Agreements or arrangements — CRTC and Commissioner of Competition**

~~115~~118 (1) The Commissioner may enter into agreements or arrangements with the Canadian Radio-television and Telecommunications Commission or the Commissioner of Competition in order to

- (a) undertake and publish research on issues of mutual interest; and

- (b) develop procedures for disclosing information referred to in subsection (2).

### **Disclosure of information**

(2) The Commissioner may, in accordance with any procedure established under paragraph (1)(b), disclose information, other than information the Commissioner has received under section 10 or paragraph ~~109~~[110\(1\)](#)(e), to the Canadian Radio-television and Telecommunications Commission or the Commissioner of Competition if the information is relevant to their powers, duties or functions.

### **Purpose and confidentiality**

(3) The procedures referred to in paragraph (1)(b) must

- (a) restrict the use of the information to the purpose for which it was originally disclosed; and
- (b) stipulate that the information be treated in a confidential manner and not be further disclosed without the express consent of the Commissioner.

### **Consultations with provinces**

~~116~~[119](#) (1) If the Commissioner considers it appropriate to do so, or on the request of an interested person, the Commissioner 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 those of the Commissioner with respect to the protection of personal information.

### **Agreements or arrangements with provinces**

(2) The Commissioner may enter into agreements or arrangements with any person referred to in subsection (1) in order to

- (a) coordinate the activities of their offices and the office of the Commissioner, including to provide for mechanisms for the handling of any complaint in which they are mutually interested;
- (b) undertake and publish research or develop and publish guidelines or other documents related to the protection of personal information;
- (c) develop model contracts or other documents related to the protection of personal information that is collected, used or disclosed interprovincially or internationally; and
- (d) develop procedures for disclosing information referred to in subsection (3).

### **Disclosure of information to provinces**

(3) The Commissioner may, in accordance with any procedure established under paragraph (2)(d), disclose information, other than information the Commissioner has received under section 10 or paragraph ~~109~~[110\(1\)](#)(e), to any person referred to in subsection (1), if the information

(a) could be relevant to an ongoing or potential investigation of a complaint, inquiry or audit under this Act or provincial legislation that has objectives that are similar to this Act; or

(b) could assist the Commissioner or that person in the exercise of their powers or the performance of their duties or functions with respect to the protection of personal information.

### **Purpose and confidentiality**

(4) The procedures referred to in paragraph (2)(d) must

(a) restrict the use of the information to the purpose for which it was originally disclosed; and

(b) stipulate that the information be treated in a confidential manner and not be further disclosed without the express consent of the Commissioner.

### **Disclosure of information to foreign state**

~~117~~120 (1) Subject to subsection (3), the Commissioner may, in accordance with any procedure established under paragraph (4)(b), disclose information referred to in subsection (2), other than information the Commissioner has received under section 10 or paragraph ~~109~~110(1)(e), that has come to the Commissioner's knowledge as a result of the exercise of any of the Commissioner's powers or the performance of any of the Commissioner's duties and functions under this Act to any person or body who, under the legislation of a foreign state, has

(a) powers, duties and functions similar to those of the Commissioner with respect to the protection of personal information; or

(b) responsibilities that relate to conduct that is substantially similar to conduct that would be in contravention of this Act.

### **Information that can be disclosed**

(2) The information that the Commissioner is authorized to disclose under subsection (1) is information that the Commissioner believes

(a) would be relevant to an ongoing or potential 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 this Act; or

(b) is necessary to disclose in order to obtain from the person or body information that may be useful to an ongoing or potential investigation, inquiry or audit under this Act.

### **Written arrangements**

(3) The Commissioner may only disclose information to the person or body referred to in subsection (1) if the Commissioner has entered into a written arrangement with that person or body that

- (a) limits the information to be disclosed to that which is necessary for the purpose set out in paragraph (2)(a) or (b);
- (b) restricts the use of the information to the purpose for which it was originally disclosed; and
- (c) stipulates that the information be treated in a confidential manner and not be further disclosed without the express consent of the Commissioner.

### **Arrangements**

(4) The Commissioner may enter into arrangements with one or more persons or bodies referred to in subsection (1) in order to

- (a) provide for cooperation with respect to the enforcement of laws protecting personal information, including the disclosure of information referred to in subsection (2) and the provision of mechanisms for the handling of any complaint in which they are mutually interested;
- (b) establish procedures for disclosing information referred to in subsection (2);
- (c) develop recommendations, resolutions, rules, standards or other documents with respect to the protection of personal information;
- (d) undertake and publish research related to the protection of personal information;
- (e) share knowledge and expertise by different means, including through staff exchanges; or
- (f) identify issues of mutual interest and determine priorities pertaining to the protection of personal information.

### **Annual report**

**4862** **121** (1) The Commissioner must, within three months after the end of each financial year, cause to be tabled in each House of Parliament a report concerning the application of this Act, the extent to which the provinces have enacted legislation that is substantially similar to this Act and the application of any such legislation.

### **Consultation**

(2) Before preparing the report, the Commissioner must consult with those persons in the provinces who, in the Commissioner's opinion, are in a position to assist the Commissioner in making a report respecting personal information that is collected, used or disclosed interprovincially or internationally.

General

### **Regulations**

**119122** (1) The Governor in Council may make regulations for carrying out the purposes and provisions of this Act, including regulations

- (a) respecting the scope of any of the activities set out in paragraphs 18(2)(a) to (e), including specifying activities that are excluded from the ~~activities set out in those paragraphs~~application of this Act;
- (b) specifying what is a government institution or part of a government institution for the purposes of any provision of this Act;
- (c) specifying information for the purpose of section 51;
- (d) specifying information to be kept and maintained under subsection 60(1); and
- (e) prescribing anything that by this Act is to be prescribed.

### Orders

(2) The Governor in Council may, by order,

- (a) provide that this Act is binding on any agent of Her Majesty in right of Canada to which the *Privacy Act* does not apply;
- (b) if satisfied that legislation of a province that is substantially similar to this Act 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 this Act in respect of the collection, use or disclosure of personal information that occurs within that province; and
- (c) amend the schedule by adding or deleting, in column 1, a reference to an organization or by adding or deleting, in column 2, the description of personal information in relation to an organization in column 1.

### Regulations — substantially similar provincial legislation

(3) The Governor in Council may make regulations establishing

- (a) criteria that are to be applied in making a determination under paragraph (2)(b) that provincial legislation is substantially similar to this Act, or in reconsidering that determination; and
- (b) the process for making or reconsidering that determination.

### Data mobility frameworks

**120123** The Governor in Council may make regulations respecting the disclosure of personal information under section 72, including regulations

- (a) respecting data mobility frameworks ~~that provide for~~and prescribing

- (i) safeguards that must be put in place by organizations to enable the secure disclosure of personal information under section 72 and the collection of that information, and
  - (ii) parameters for the technical means for ensuring interoperability in respect of the disclosure and collection of that information;
- (b) specifying organizations that are subject to a data mobility framework; and
- (c) providing for exceptions to the requirement to disclose personal information under that section, including exceptions related to the protection of proprietary or confidential commercial information.

### **Distinguishing — classes**

**121124** Regulations made under subsection ~~119(1)~~122(1) or section ~~120~~123 may distinguish among different classes of activities, government institutions or parts of government institutions, information, organizations or entities.

### **Regulations — codes of conduct and certification programs**

**122125** The Minister may make regulations

- (a) ~~providing for~~respecting the ~~manner of~~making of an application under subsection 76(2);
- (b) setting out criteria for the purpose of subsection 76(3);
- (c) respecting the reconsideration of a determination made under subsection 76(3);
- (d) ~~providing for~~respecting the ~~manner of~~making of an application under subsection 77(1);
- (e) providing for anything else that must be included in a certification program for the purpose of paragraph 77(1)(f);
- (f) setting out criteria for the purpose of subsection 77(2);
- (g) respecting the reconsideration of a determination made under subsection 77(2);
- (h) specifying, for the purpose of section 78, the time for responding to an application;
- (i) respecting the criteria for and the manner and the circumstances in which a recommendation may be made under paragraph 81(c);
- (j) respecting the criteria for and the manner and the circumstances in which an approval may be revoked under paragraph 81(e); and
- (k) respecting record-keeping and reporting obligations of an entity that operates an approved certification program, including obligations to provide reports to the Commissioner in respect of an approved certification program.



## **Whistleblowing**

**123126** (1) Any person who has reasonable grounds to believe that a person has contravened or intends to contravene Part 1 may notify the Commissioner of the particulars of the matter and may request that their identity be kept confidential with respect to the notification.

## **Confidentiality**

(2) The Commissioner must keep confidential the identity of a person who has notified the Commissioner under subsection (1) and to whom an assurance of confidentiality has been provided by the Commissioner.

## **Prohibition**

**124127** (1) 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

(a) the employee, acting in good faith and on the basis of reasonable belief, has disclosed to the Commissioner that the employer or any other person has contravened or intends to contravene Part 1;

(b) the employee, acting in good faith and on the basis of reasonable belief, has refused or stated an intention of refusing to do anything that is a contravention of Part 1;

(c) the employee, acting in good faith and on the basis of reasonable belief, has done or stated an intention of doing anything that is required to be done in order that Part 1 not be contravened; or

(d) the employer believes that the employee will do anything referred to in paragraph (a), (b) or (c).

## **Saving**

(2) Nothing in this section impairs any right of an employee, either at law or under an employment contract or collective agreement.

## **Definitions of *employee* and *employer***

(3) In this section, *employee* includes an independent contractor and *employer* has a corresponding meaning.

## **Offence and punishment**

**125128** Every organization that knowingly contravenes section 58, subsection 60(1), section 69 or 75 or subsection ~~124(1)~~**127(1)** or an order under subsection ~~92(2)~~**293(2)** or that obstructs the Commissioner or the Commissioner's delegate in the investigation of a complaint, in conducting an inquiry or in carrying out an audit is

(a) guilty of an indictable offence and liable to a fine not exceeding the higher of \$25,000,000 and 5% of the organization's gross global revenue in its financial year before the one in which the organization is sentenced; or

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

### **Review by parliamentary committee**

**126129** (1) Five years after the day on which this section comes into force, and every five years after that, a comprehensive review of the provisions and operation of this Act is to be commenced by a committee of the Senate, of the House of Commons or of both Houses of Parliament that may be designated or established by the Senate, the House of Commons or both Houses of Parliament, as the case may be, for that purpose.

### **Report**

(2) Within one year, or any further time that is authorized by the Senate, the House of Commons or both Houses of Parliament, as the case may be, after the day on which the review is commenced, the committee must submit a report on that review to the Senate, the House of Commons or both Houses of Parliament, as the case may be, together with a statement of any changes recommended by the committee.

## **PART 3**

### **Coming into Force**

#### **Order in council**

**130** (1) Subject to subsections (2) and (3), this Act comes into force on the day on which section 3 of the *Digital Charter Implementation Act, 2022* comes into force.

#### **Order in council**

**(2)** Sections 72 and 123 come into force on a day to be fixed by order of the Governor in Council.

#### **Order in council**

**(3)** Sections 76 to 81, paragraph 83(1)(d), subsection 94(3) and section 125 come into force on a day to be fixed by order of the Governor in Council.

Consequential and Related Amendments

2000, c. 5

Personal Information Protection and Electronic Documents Act

**3 The long title of the *Personal Information Protection and Electronic Documents Act* is replaced by the following:**

An Act to provide for the use of electronic means to communicate or record information or transactions

2000, c. 17, par. 97(1)(b) and (d); 2001, c. 41, ss. 81, 82 and 103; 2002, c. 8, par. 183(1)(r); 2004, c. 15, s. 98; 2005, c. 46, s. 57; 2006, c. 9, s. 223; 2010, c. 23, ss. 82 to 84, 86(2) and 87; 2015, c. 32, ss. 2 to 7, 8(F), 9 to 17, 18(1) and (2)(E), 19, 20(1) and (2)(E), 21 to 24 and 26(2) and (3), c. 36, s. 164 and 165; 2019, c. 18, s. 61

**4 Sections 1 to 30 of the Act are replaced by the following:**

**Short title**

**1** This Act may be cited as the *Electronic Documents Act*.

**5 Section 31 of the Act is amended by adding the following after subsection (2):**

**Designation of Minister**

**(3)** The Governor in Council may, by order, designate a member of the Queen's Privy Council for Canada as the Minister responsible for this Act.

**6 Parts 3 to 5 of the Act are repealed.**

**7 Schedule 1 to the Act is repealed.**

2015, c. 36, s. 166

**8 Schedule 4 to the Act is repealed.**

R.S., c. A-1

Access to Information Act

2015, c. 32, s. 25

**9 (1) Schedule II to the *Access to Information Act* is amended by striking out the reference to**

Personal Information Protection and Electronic Documents Act

**and the corresponding reference to "subsection 20(1.1)".**

**(2) Schedule II to the Act is amended by adding, in alphabetical order, a reference to**

Consumer Privacy Protection Act

and a corresponding reference to "subsection ~~112(2)~~[113\(2\)](#)".

R.S., c. A-2

Aeronautics Act

2011, c. 9, s. 2(1)

**10 Subsection 4.83(1) of the *Aeronautics Act* is replaced by the following:**

**Foreign states requiring information**

**4.83 (1)** Despite Part 1 of the *Consumer Privacy Protection Act*, to the extent that that Part relates to obligations relating to the disclosure of information, an operator of an aircraft departing from Canada that is due to land in a foreign state or fly over the United States and land outside Canada or of a Canadian aircraft departing from any place outside Canada that is due to land in a foreign state or fly over the United States may, in accordance with the regulations, provide to a competent authority in that foreign state any information that is in the operator's control relating to persons on board or expected to be on board the aircraft and that is required by the laws of the foreign state.

R.S., c. C-5

Canada Evidence Act

2001, c. 41, s. 44

**11 Item 14 of the schedule to the *Canada Evidence Act* is replaced by the following:**

**14** The Privacy Commissioner, for the purposes of the *Consumer Privacy Protection Act*

2001, c. 41, s. 44

**12 Item 17 of the schedule to the Act is replaced by the following:**

**17** The Personal Information and Data Protection Tribunal, for the purposes of the *Consumer Privacy Protection Act*

R.S., c. C-22

Canadian Radio-television and Telecommunications Commission Act

**13 The *Canadian Radio-television and Telecommunications Commission Act* is amended by adding the following after section 12:**

**Agreements or arrangements — Privacy Commissioner**

**12.1 (1)** The Commission may enter into an agreement or arrangement with the Privacy Commissioner in order to

- (a) undertake and publish research on issues of mutual interest; and
- (b) develop procedures for disclosing information referred to in subsection (2).

**Disclosure of information**

(2) The Commission may, in accordance with any procedure established under paragraph (1)(b), disclose information to the Privacy Commissioner if the information is relevant to the Commissioner's powers, duties or functions under the *Consumer Privacy Protection Act*.

**Purpose and confidentiality**

- (3) The procedures referred to in paragraph (1)(b) shall
  - (a) restrict the use of the information to the purpose for which it was originally disclosed; and
  - (b) stipulate that the information be treated in a confidential manner and not be further disclosed without the express consent of the Commission.

R.S., c. C-34~~;~~; R.S., c. 19 (2nd Supp.), s. 19

Competition Act

**14 The *Competition Act* is amended by adding the following after section 29.2:**

**Agreements or arrangements — Privacy Commissioner**

**29.3 (1)** Despite subsection 29(1), the Commissioner may enter into an agreement or arrangement with the Privacy Commissioner in order to

- (a) undertake and publish research on issues of mutual interest; and
- (b) develop procedures for disclosing information referred to in subsection (2).

**Disclosure of information**

(2) The Commissioner may, in accordance with any procedure established under paragraph (1)(b), disclose information to the Privacy Commissioner if the information is relevant to the Privacy Commissioner's powers, duties or functions under the *Consumer Privacy Protection Act*.

**Purpose and confidentiality**

- (3) The procedures referred to in paragraph (1)(b) shall
  - (a) restrict the use of the information to the purpose for which it was originally disclosed; and

(b) stipulate that the information be treated in a confidential manner and not be further disclosed without the express consent of the Commissioner.

R.S., c. C-44; 1994, c. 24, s. 1(F)

Canada Business Corporations Act

2018, c. 27, s. 183

**15 Subsection 21.1(5) of the *Canada Business Corporations Act* is replaced by the following:**

**Disposal of personal information**

(5) Within one year after the sixth anniversary of the day on which an individual ceases to be an individual with significant control over the corporation, the corporation shall — subject to any other Act of Parliament and to any Act of the legislature of a province that provides for a longer retention period — dispose of any of that individual's *personal information*, as defined in [section 2](#)[subsection 2\(1\)](#) of the *Consumer Privacy Protection Act*, that is recorded in the register.

[1993, c. 38](#)

[Telecommunications Act](#)

[2010, c. 23, s. 88\(1\)](#)

**[16 \(1\) Subsection 39\(2\) of the \*Telecommunications Act\* is replaced by the following:](#)**

**[Information not to be disclosed](#)**

[\(2\) Subject to subsections \(4\), \(5\) and \(5.1\) to \(6\), if a person designates information as confidential and the designation is not withdrawn by that person, no person described in subsection \(3\) shall knowingly disclose the information, or knowingly allow it to be disclosed, to any other person in any manner that is calculated or likely to make it available for the use of any person who may benefit from the information or use the information to the detriment of any person to whose business or affairs the information relates.](#)

**[\(2\) Section 39 of the Act is amended by adding the following after subsection \(5.1\):](#)**

**[Disclosure to Privacy Commissioner](#)**

[\(5.2\) The Commission may disclose designated information obtained by it in the exercise of its powers or the performance of its duties or functions under this Act to the Privacy Commissioner in accordance with section 12.1 of the \*Canadian Radio-television and Telecommunications Commission Act\*.](#)

2005, c. 46

Public Servants Disclosure Protection Act

**1617** Paragraph 15(a) of the *Public Servants Disclosure Protection Act* is replaced by the following:

- (a) Part 1 of the *Consumer Privacy Protection Act*, to the extent that that Part relates to obligations relating to the disclosure of information; and

**1718** Subsection 16(1.1) of the Act is replaced by the following:

#### Limitation

(1.1) Subsection (1) does not apply in respect of information the disclosure of which is subject to any restriction created by or under any Act of Parliament, including the *Consumer Privacy Protection Act*.

**1819** Section 50 of the Act is replaced by the following:

#### Personal information

50 Despite Part 1 of the *Consumer Privacy Protection Act*, to the extent that that Part relates to obligations relating to the disclosure of information, and despite any other Act of Parliament that restricts the disclosure of information, a report by a chief executive in response to recommendations made by the Commissioner to the chief executive under this Act may include *personal information* within the meaning of ~~section 2~~subsection 2(1) of that Act, or section 3 of the *Privacy Act*, depending on which of those Acts applies to the portion of the public sector for which the chief executive is responsible.

2010, c. 23

Chapter 23 of the Statutes of Canada, 2010

**1920** Section 2 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* is replaced by the following:

#### Precedence of this Act

2 In the event of a conflict between a provision of this Act and a provision of the *Consumer Privacy Protection Act*, the provision of this Act operates despite the provision of that Act, to the extent of the conflict.

**2021** Paragraph 20(3)(c) of the Act is replaced by the following:

- (c) the person's history with respect to
  - (i) any previous violation of this Act,
  - (ii) any previous conduct that is reviewable under section 74.011 of the *Competition Act*,

(iii) any previous contravention of section 5 of the *Personal Information Protection and Electronic Documents Act*, as it read immediately before the day on which section 4 of the *Digital Charter Implementation Act*, ~~2020~~2022 comes into force, that relates to a collection or use described in subsection 7.1(2) or (3) of that Act, and

(iv) any previous contravention of Part 1 of the *Consumer Privacy Protection Act* that relates to a collection or use described in subsection 52(2) or (3) of that Act;

**~~2122~~ (1) Subsection 47(1) of the Act is replaced by the following:**

**Application**

**47 (1)** A person who alleges that they are affected by an act or omission that constitutes a contravention of any of sections 6 to 9 of this Act or a contravention of Part 1 of the *Consumer Privacy Protection Act* that relates to a collection or use described in subsection 52(2) or (3) of that Act — or that constitutes conduct that is reviewable under section 74.011 of the *Competition Act* — may apply to a court of competent jurisdiction for an order under section 51 against one or more persons whom they allege have committed the act or omission or whom they allege are liable for the contravention or reviewable conduct by reason of section 52 or 53.

**(2) Subsection 47(4) of the Act is replaced by the following:**

**Notice**

**(4)** The applicant must, without delay, serve a copy of the application on every person against whom an order is sought, on the Commission if the application identifies a contravention of this Act, on the Commissioner of Competition if the application identifies conduct that is reviewable under section 74.011 of the *Competition Act* and on the Privacy Commissioner if the application identifies a contravention of the *Consumer Privacy Protection Act*.

**~~2223~~ Paragraph 50(c) of the Act is replaced by the following:**

(c) the Privacy Commissioner, if the application identifies a contravention of the *Consumer Privacy Protection Act*.

**~~2324~~ (1) Subparagraph 51(1)(b)(vi) of the Act is replaced by the following:**

(vi) in the case of a contravention of Part 1 of the *Consumer Privacy Protection Act* that relates to a collection or use described in subsection 52(2) or (3) of that Act, \$1,000,000 for each day on which a                    contravention occurred, and

**(2) Subsection 51(2) of the Act is replaced by the following:**

**Purpose of order**

**(2)** The purpose of an order under paragraph (1)(b) is to promote compliance with this Act, the *Consumer Privacy Protection Act* or the *Competition Act*, as the case may be, and not to punish.



**(3) Paragraph 51(3)(c) of the Act is replaced by the following:**

(c) the person's history, or each person's history, as the case may be, with respect to

(i) any previous contravention of this Act,

(ii) any previous contravention of section 5 of the *Personal Information Protection and Electronic Documents Act*, as it read immediately before the day on which section 4 of the *Digital Charter Implementation Act*, ~~2020~~2022 comes into force, that relates to a collection or use described in subsection 7.1(2) or (3) of that Act,

(iii) any previous contravention of Part 1 of the *Consumer Privacy Protection Act* that relates to a collection or use described in subsection 52(2) or (3) of that Act, and

(iv) any previous conduct that is reviewable under section 74.011 of the *Competition Act*;

**~~2425~~ Sections 52 to 54 of the Act are replaced by the following:**

**Directors and officers of corporations**

**52** An officer, director or agent or mandatary of a corporation that commits a contravention of any of sections 6 to 9 of this Act or of Part 1 of the *Consumer Privacy Protection Act* that relates to a collection or use described in 1 subsection 52(2) or (3) of that Act, or that engages in conduct that is reviewable under section 74.011 of the *Competition Act*, is liable for the contravention or reviewable conduct, as the case may be, if they directed, authorized, assented to, acquiesced in or participated in the commission of that contravention, or engaged in that conduct, whether or not the corporation is proceeded against.

**Vicarious liability**

**53** A person is liable for a contravention of any of sections 6 to 9 of this Act or of Part 1 of the *Consumer Privacy Protection Act* that relates to a collection or use described in subsection 52(2) or (3) of that Act, or for conduct that is reviewable under section 74.011 of the *Competition Act*, that is committed or engaged in, as the case may be, by their employee acting within the scope of their employment or their agent or mandatary acting within the scope of their authority, whether or not the employee or agent or mandatary is identified or proceeded against.

**Defence**

**54 (1)** A person must not be found to have committed a contravention of any of sections 6 to 9 of this Act or of Part 1 of the *Consumer Privacy Protection Act* that relates to a collection or use described in subsection 52(2) or (3) of that Act, or to have engaged in conduct that is reviewable under section 74.011 of the *Competition Act*, if they establish that they exercised due diligence to prevent the contravention or conduct, as the case may be.

**Common law principles**

(2) Every rule and principle of the common law that makes any circumstance a justification or excuse in relation to a charge for an offence applies in respect of a contravention or conduct referred to in subsection (1), to the extent that it is not inconsistent with this Act or the Consumer Privacy Protection Act or the Competition Act, as the case may be.

**2526** (1) The portion of section 56 of the Act before paragraph (a) is replaced by the following:

#### **Disclosure by an organization**

56 Any organization to which the Consumer Privacy Protection Act applies may on its own initiative disclose to the Commission, the Commissioner of Competition or the Privacy Commissioner any information in its possession that it believes relates to

(2) Subparagraph 56(a)(iii) of the Act is replaced by the following:

(iii) Part 1 of the Consumer Privacy Protection Act, which contravention relates to a collection or use described in subsection 52(2) or (3) of that Act, or

**2627** Section 57 of the Act is replaced by the following:

#### **Consultation**

57 The Commission, the Commissioner of Competition and the Privacy Commissioner must consult with each other to the extent that they consider appropriate to ensure the effective regulation, under this Act, the Competition Act, the Consumer Privacy Protection Act and the Telecommunications Act, of commercial conduct that discourages the use of electronic means to carry out commercial activities, and to coordinate their activities under those Acts as they relate to the regulation of that type of conduct.

**2728** (1) Paragraph 58(1)(a) of the Act is replaced by the following:

(a) to the Privacy Commissioner, if the Commission believes that the information relates to the exercise of the Privacy Commissioner's powers or the performance of the Privacy Commissioner's duties or functions under the Consumer Privacy Protection Act in respect of a collection or use described in subsection 52(2) or (3) of that Act; and

(2) Paragraph 58(2)(a) of the Act is replaced by the following:

(a) to the Privacy Commissioner, if the Commissioner of Competition believes that the information relates to the exercise of the Privacy Commissioner's powers or the performance of the Privacy Commissioner's duties or functions under the Consumer Privacy Protection Act in respect of a collection or use described in subsection 52(2) or (3) of that Act; and

(3) The portion of subsection 58(3) of the Act before paragraph (a) is replaced by the following:

#### **Disclosure by Privacy Commissioner**

(3) The Privacy Commissioner may disclose information obtained by the Privacy Commissioner in the exercise of the Privacy Commissioner's powers or the performance of the Privacy Commissioner's duties or functions under the *Consumer Privacy Protection Act* if the information relates to a collection or use described in subsection 52(2) or (3) of that Act or to an act alleged in a complaint in respect of which the Privacy Commissioner decides, under ~~subsection 83(2) or 85(2)~~section 84 of that Act, to not conduct an investigation or to discontinue an investigation,

**2829 Subsection 59(3) of the Act is replaced by the following:**

#### **Use of information by Privacy Commissioner**

(3) The Privacy Commissioner may use the information that is disclosed to the Privacy Commissioner under paragraph 58(1)(a) or (2)(a) only for the purpose of exercising the Privacy Commissioner's powers or performing the Privacy Commissioner's duties or functions under the *Consumer Privacy Protection Act* in respect of a collection or use described in subsection 52(2) or (3) of that Act.

**2930 (1) Subparagraph 60(1)(a)(ii) of the Act is replaced by the following:**

(ii) conduct that contravenes Part 1 of the *Consumer Privacy Protection Act* and that relates to a collection or use described in subsection 52(2) or (3) of that Act,

**(2) Subparagraph 60(1)(b)(iii) of the Act is replaced by the following:**

(~~iii~~y) the exercise by the Privacy Commissioner of the Privacy Commissioner's powers or the performance of the Privacy Commissioner's duties or functions under the *Consumer Privacy Protection Act* in respect of a collection or use described in subsection 52(2) or (3) of that Act, or

**3031 Section 61 of the Act is replaced by the following:**

#### **Reports to Minister of Industry**

**61** The Commission, the Commissioner of Competition and the Privacy Commissioner must provide the Minister of Industry with any reports that the Minister requests for the purpose of coordinating the implementation of sections 6 to 9 of this Act, sections 52.01 and 74.011 of the *Competition Act* and section 52 of the *Consumer Privacy Protection Act*.

2018, c. 10

Transportation Modernization Act

**3132 Section 62 of the *Transportation Modernization Act* is amended by replacing the subsection 17.91(4) that it enacts with the following:**

#### ***Consumer Privacy Protection Act* and provincial legislation**

(4) A company that collects, uses or communicates information under this section, section 17.31 or 17.94, subsection 28(1.1) or 36(2) or regulations made under section 17.95 may do so

(a) despite Part 1 of the *Consumer Privacy Protection Act*, to the extent that that Part relates to obligations relating to the collection, use, disclosure, retention and disposal of information; and

(b) despite any provision of provincial legislation that is substantially similar to that Act and that limits the collection, use, communication or preservation of information.

## Terminology

### Replacement of "*Personal Information Protection and Electronic Documents Act*"

**3233** Every reference to the "*Personal Information Protection and Electronic Documents Act*" is replaced by a reference to the "*Electronic Documents Act*" in the following provisions:

- (a) the definition *secure electronic signature* in section 31.8 of the *Canada Evidence Act*;
- (b) subsection 95(2) of the *Canadian Forces Superannuation Act*;
- (c) subsections 252.6(2) and (3) of the *Canada 5 Business Corporations Act*;
- (d) subsection 74(2) of the *Public Service Superannuation Act*;
- (e) subsection 44(2) of the *Royal Canadian Mounted Police Superannuation Act*;
- (f) subparagraph 205.124(1)(u)(ii) of the *Canada–Newfoundland and Labrador Atlantic Accord Implementation Act*;
- (g) subparagraph 210.126(1)(u)(ii) of the *Canada–Nova Scotia Offshore Petroleum Resources Accord Implementation Act*;
- (h) subsections 539.1(2) and (3) of the *Trust and Loan Companies Act*;
- (i) subsections 1001(2) and (3) of the *Bank Act*;
- (j) subsections 1043(2) and (3) of the *Insurance Companies Act*;
- (k) subsections 487.1(2) and (3) of the *Cooperative Credit Associations Act*;
- (l) subsections 361.6(2) and (3) of the *Canada Cooperatives Act*; and
- (m) subsections 269(2) and (3) of the *Canada Not-for-profit Corporations Act*.

## Transitional Provisions

## Definitions

**3334** (1) The following definitions apply in this section.

*former Act* means the *Personal Information Protection and Electronic Documents Act*, as it read immediately before the day on which section 82 of the *Consumer Privacy Protection Act*, enacted by section 2, comes into force.

*new Act* means the *Consumer Privacy Protection Act*.

#### Pending complaints

(2) If a complaint was filed or initiated under section 11 of the former Act before the day on which section 82 of the new Act comes into force and it has not been dealt with or disposed of on that day, the complaint is to be dealt with and disposed of in accordance with the former Act. However, if the Privacy Commissioner has reasonable grounds to believe that the contravention that is alleged in the complaint is continuing after that day, the complaint is to be dealt with and disposed of in accordance with the new Act.

#### Contraventions before coming into force

(3) If a complaint is filed or initiated on or after the day on which section 82 of the new Act comes into force in respect of a contravention that is alleged to have occurred before that day, the complaint is to be dealt with and disposed of in accordance with the former Act. However, if the Privacy Commissioner has reasonable grounds to believe that the contravention that is alleged in the complaint is continuing after that day, the complaint is to be dealt with and disposed of in accordance with the new Act.

#### Coordinating Amendments

#### Bill C-11

35 If Bill C-11, introduced in the 1st session of the 44th Parliament and entitled the *Online Streaming Act*, receives royal assent, then on the first day on which both section 22 of that Act and section 13 of this Act are in force,

(a) subsection 25.3(2) of the *Broadcasting Act* is replaced by the following:

#### Information not to be disclosed

(2) Subject to subsections (4) to (5.1) and (7), if a person designates information as confidential and the designation is not withdrawn by that person, no person described in subsection (3) shall knowingly disclose the information, or knowingly allow it to be disclosed, to any other person in any manner that is intended or likely to make it available for the use of any person who may benefit from the information or use it to the detriment of any person to whose business or affairs the information relates.

(b) section 25.3 of the *Broadcasting Act*, as enacted by that section 22, is amended by adding the following after subsection (5):

## Disclosure to Privacy Commissioner

(5.1) The Commission may disclose designated information obtained by it in the exercise of its powers or the performance of its duties or functions under this Act to the Privacy Commissioner in accordance with section 12.1 of the *Canadian Radio-television and Telecommunications Commission Act*.

2018, c. 10

**3436** (1) In this section, *other Act* means the *Transportation Modernization Act*.

(2) If section 62 of the other Act comes into force before section 2 of this Act, then

(a) section ~~31~~32 of this Act is repealed; and

(b) on the coming into force of section 2 of this Act, subsection 17.91(4) of the *Railway Safety Act* is replaced by the following:

### ***Consumer Privacy Protection Act and provincial legislation***

(4) A company that collects, uses or communicates information under this section, section 17.31 or 17.94, subsection 28(1.1) or 36(2) or regulations made under section 17.95 may do so

(a) despite Part 1 of the *Consumer Privacy Protection Act*, to the extent that that Part relates to obligations relating to the collection, use, disclosure, retention and disposal of information; and

(b) despite any provision of provincial legislation that is substantially similar to that Act and that limits the collection, use, communication or preservation of information.

(3) If section 62 of the other Act comes into force on the same day as section ~~31~~32 of this Act, then that section ~~31~~32 is deemed to have come into force before that section 62.

## **PART 2**

### **Personal Information and Data Protection Tribunal Act**

Enactment of Act

#### **Enactment**

**3537** The *Personal Information and Data Protection Tribunal Act* is enacted as follows:

An Act to establish the Personal Information and Data Protection Tribunal

#### **Short title**

1 This Act may be cited as the *Personal Information and Data Protection Tribunal Act*.

#### **Definition of *Minister***

2 In this Act, *Minister* means the member of the Queen's Privy Council for Canada designated under section 3 or, if no member is designated, the Minister of Industry.

### **Order designating Minister**

3 The Governor in Council may, by order, designate any member of the Queen's Privy Council for Canada to be the Minister for the purposes of this Act.

### **Establishment**

4 A tribunal to be called the Personal Information and Data Protection Tribunal ("the Tribunal") is established.

### **Jurisdiction**

5 The Tribunal has jurisdiction in respect of all appeals that may be made under section ~~100~~101 or ~~101~~102 of the *Consumer Privacy Protection Act* and in respect of the imposition of penalties under section ~~94~~95 of that Act.

### **Members**

6 (1) The Tribunal consists of three to six members to be appointed by the Governor in Council on the recommendation of the Minister.

### **Full- or part-time members**

(2) Members may be appointed as full-time or part-time members.

### **Full-time occupation**

(3) Full-time members must devote the whole of their time to the performance of their duties and functions under this Act.

### **Experience**

(4) At least ~~one~~three of the members must have experience in the field of information and privacy law.

### **Chairperson and Vice-Chairperson**

7 The Governor in Council must designate one member as Chairperson of the Tribunal and may designate one member as Vice-Chairperson. The Chairperson must be a full-time member.

### **Duties of Chairperson**

8 (1) The Chairperson has supervision over, and direction of the work of the Tribunal, including

(a) the distribution of work among members and the assignment of members to hear matters brought before the Tribunal and, if the Chairperson considers it appropriate for matters to be heard by panels, the assignment of members to panels and to preside over panels; and

(b) the conduct of the work of the Tribunal and the management of its internal affairs.

### **Acting Chairperson**

(2) In the event of the absence or incapacity of the Chairperson or if the office of Chairperson is vacant, the Vice-Chairperson acts as Chairperson.

### **Acting Chairperson**

9 In the event of the absence or incapacity of the Chairperson and the Vice-Chairperson or if both of those offices are vacant, a member of the Tribunal designated by the Minister acts as Chairperson. The designated member is not however authorized to act as Chairperson for a period of more than 90 days without the approval of the Governor in Council.

### **Term of office**

10 (1) A member is to be appointed to hold office during good behaviour for a term not exceeding five years and may be removed for cause by the Governor in Council.

### **Reappointment**

(2) A member is eligible to be reappointed for one or more terms not exceeding three years each.

### **Disposition after expiry of appointment**

(3) A member whose appointment expires may, at the request of the Chairperson and for a period of not more than six months, make or take part in a decision on a matter that they heard as a member. For that purpose, the former member is deemed to be a part-time member.

### **Remuneration**

11 (1) Members are to receive the remuneration that is fixed by the Governor in Council.

### **Expenses**

(2) Each member is entitled to be paid reasonable travel and living expenses incurred while absent in the course of their duties from, in the case of a full-time member, their ordinary place of work and, in the case of a part-time member, their ordinary place of residence.

### **Status**

(3) Members are deemed to be employees for the purposes of the *Government Employees Compensation Act* and to be employed in the federal public administration for the purposes of any regulations made under section 9 of the *Aeronautics Act*.



### ***Public Service Superannuation Act***

(4) Full-time members are also deemed to be persons employed in the public service for the purposes of the *Public Service Superannuation Act*.

#### **Inconsistent interests**

**12** If a member who is assigned to hear or is hearing any matter before the Tribunal, either alone or as a member of a panel, holds any pecuniary or other interest that could be inconsistent with the proper performance of their duties and functions in relation to the matter, the member must disclose the interest to the Chairperson without delay.

#### **Principal office**

**13** The principal office of the Tribunal must be in a place in Canada that is designated by the Governor in Council or, if no place is designated, in the National Capital Region described in the schedule to the *National Capital Act*.

#### **Sittings**

**14** The Tribunal is to sit at those times and places in Canada and in the manner that the Chairperson considers necessary for the proper performance of its duties and functions.

#### **Nature of hearings**

**15 (1)** Subject to subsection (2), the Tribunal is not bound by any legal or technical rules of evidence in conducting a hearing in relation to any matter that comes before it and it must deal with all matters as informally and expeditiously as the circumstances and considerations of fairness and natural justice permit.

#### **Restriction**

(2) The Tribunal must not receive or accept as evidence anything that would be inadmissible in a court by reason of any privilege under the law of evidence.

#### **Appearance**

(3) A party to a proceeding before the Tribunal may appear in person or be represented by another person, including legal counsel.

#### **Private hearings**

(4) Hearings must be held in public. However, the Tribunal may hold all or any part of a hearing in private if it is of the opinion that

- (a) a public hearing would not be in the public interest; or

(b) confidential information may be disclosed and the desirability of ensuring that the information is not publicly disclosed outweighs the desirability of adhering to the principle that hearings be open to the public.

### **Standard of proof**

(5) In any proceeding before the Tribunal, a party that has the burden of proof discharges it by proof on the balance of probabilities.

### **Decision of panel**

(6) A decision of the majority of the members of a panel referred to in paragraph 8(1)(a) is a decision of the Tribunal.

### **Powers**

~~16 The Tribunal and each of its members have all the powers of a commissioner under Part I of the *Inquiries Act* and the power to make interim~~

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

### **Enforcement of decisions**

(2) Any decision of the Tribunal may, for the purposes of its enforcement, be made an order of the Federal Court or of any superior court and is enforceable in the same manner as an order of the court.

### **Procedure**

(3) To make a decision of the Tribunal an order of a court, the usual practice and procedure of the court in such matters may be followed or a certified copy of the decision may be filed with the registrar of the court, at which time the decision becomes an order of the court.

### **Reasons**

17 The Tribunal must provide a decision, with reasons, in writing to all parties to a proceeding.

### **Public availability — decisions**

18 (1) The Tribunal must make its decisions, and the reasons for them, publicly available in accordance with its rules.

### **Complainants**

(2) If the Tribunal makes a decision in relation to a complaint filed under the *Consumer Privacy Protection Act*, the Tribunal must not make the complainant's name or any personal information

that could be used to identify the complainant publicly available without the complainant's consent.

## **Rules**

**19 (1)** The Tribunal may, with the approval of the Governor in Council, make rules that are not inconsistent with this Act or the *Consumer Privacy Protection Act* to govern the management of its affairs and the practice and procedure in connection with matters brought before it, including rules respecting when decisions are to be made public and the factors to be taken into consideration in deciding whether to name an organization affected by a decision in the decision.

## **Public availability — rules**

(2) The Tribunal must make its rules publicly available.

## **Costs**

### **Cost**

**20 (1)** The Tribunal may, in accordance with its rules, award costs.

## **Certificate**

(2) Costs under subsection (1) that have not been paid may be certified by the Tribunal.

## **Registration of certificate**

(3) On production to the Federal Court, a certificate must be registered. When it is registered, a certificate has the same force and effect as if it were a judgment obtained in the Federal Court for a debt of the amount specified in it and all reasonable costs and charges attendant on its registration, recoverable in that Court or in any other court of competent jurisdiction.

## **Decisions final**

**21** A decision of the Tribunal is final and binding and, except for judicial review under the *Federal Courts Act*, is not subject to appeal or to review by any court.

2014, c. 20, s. 376

Related Amendment to the Administrative Tribunals Support Service of Canada Act

**3638** The schedule to the *Administrative Tribunals Support Service of Canada Act* is amended by adding the following in alphabetical order:

Personal Information and Data Protection Tribunal

## **PART 3**

### **Coming into Force**

### **Order in council**

~~37(~~

## **Artificial Intelligence and Data Act**

### **Enactment of Act**

#### **39 The Artificial Intelligence and Data Act is enacted as follows:**

An Act respecting artificial intelligence systems and data used in artificial intelligence systems

### **Short Title**

#### **Short title**

**1)** This Act may be cited as the *Artificial Intelligence and Data Act*.

### **Definitions and Application**

#### **Definitions**

**2** The following definitions apply in this Act.

*artificial intelligence system* means a technological system that, autonomously or partly autonomously, processes data related to human activities through the use of a genetic algorithm, a neural network, machine learning or another technique in order to generate content or make decisions, recommendations or predictions.

*person* includes a trust, a joint venture, a partnership, an unincorporated association and any other legal entity.

*personal information* has the meaning assigned by subsections 2(1) and (3) of the *Consumer Privacy Protection Act*.

#### **Non-application**

**3 (1)** This Act does not apply with respect to a *government institution* as defined in section 3 of the *Privacy Act*.

#### **Product, service or activity**

**(2)** This Act does not apply with respect to a product, service or activity that is under the direction or control of

- (a) the Minister of National Defence;
- (b) the Director of the Canadian Security Intelligence Service;
- (c) the Chief of the Communications Security Establishment; or
- (d) any other person who is responsible for a federal or provincial department or agency and who is prescribed by regulation.

### Regulations

(3) The Governor in Council may make regulations prescribing persons for the purpose of paragraph (2)(d).

### Purposes of Act

#### Purposes

4 The purposes of this Act are

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

## PART 1

### Regulation of Artificial Intelligence Systems in the Private Sector

#### Interpretation

#### Definitions

5 (1) The following definitions apply in this Part.

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

*confidential business information*, in respect of a person to whose business or affairs the information relates, means business information

(a) that is not publicly available;

(b) in respect of which the person has taken measures that are reasonable in the circumstances to ensure that it remains not publicly available; and

(c) that has actual or potential economic value to the person or their competitors because it is not publicly available and its disclosure would result in a material financial loss to the person or a material financial gain to their competitors.

**harm means**

(a) physical or psychological harm to an individual;

(b) damage to an individual's property; or

(c) economic loss to an individual.

**high-impact system** means an artificial intelligence system that meets the criteria for a high-impact system that are established in regulations.

**Minister** means the member of the Queen's Privy Council for Canada designated under section 31 or, if no member is so designated, the Minister of Industry.

**regulated activity** means any of the following activities carried out in the course of international or interprovincial trade and commerce:

(a) processing or making available for use any data relating to human activities for the purpose of designing, developing or using an artificial intelligence system;

(b) designing, developing or making available for use an artificial intelligence system or managing its operations.

**Person responsible**

(2) For the purposes of this Part, a person is responsible for an artificial intelligence system, including a high-impact system, if, in the course of international or interprovincial trade and commerce, they design, develop or make available for use the artificial intelligence system or manage its operation.

**Requirements**

**Anonymized data**

**6** A person who carries out any regulated activity and who processes or makes available for use anonymized data in the course of that activity must, in accordance with the regulations, establish measures with respect to

(a) the manner in which data is anonymized; and

(b) the use or management of anonymized data.

### **Assessment — high-impact system**

7 A person who is responsible for an artificial intelligence system must, in accordance with the regulations, assess whether it is a high-impact system.

### **Measures related to risks**

8 A person who is responsible for a high-impact system must, in accordance with the regulations, establish measures to identify, assess and mitigate the risks of harm or biased output that could result from the use of the system.

### **Monitoring of mitigation measures**

9 A person who is responsible for a high-impact system must, in accordance with the regulations, establish measures to monitor compliance with the mitigation measures they are required to establish under section 8 and the effectiveness of those mitigation measures.

### **Keeping general records**

10 (1) A person who carries out any regulated activity must, in accordance with the regulations, keep records describing in general terms, as the case may be,

(a) the measures they establish under sections 6, 8 and 9; and

(b) the reasons supporting their assessment under section 7.

### **Additional records**

(2) The person must, in accordance with the regulations, keep any other records in respect of the requirements under sections 6 to 9 that apply to them.

### **Publication of description — making system available for use**

11 (1) A person who makes available for use a high-impact system must, in the time and manner that may be prescribed by regulation, publish on a publicly available website a plain-language description of the system that includes an explanation of

(a) how the system is intended to be used;

(b) the types of content that it is intended to generate and the decisions, recommendations or predictions that it is intended to make;

(c) the mitigation measures established under section 8 in respect of it; and

(d) any other information that may be prescribed by regulation.

### **Publication of description — managing operation of system**

(2) A person who manages the operation of a high-impact system must, in the time and manner that may be prescribed by regulation, publish on a publicly available website a plain-language description of the system that includes an explanation of

(a) how the system is used;

(b) the types of content that it generates and the decisions, recommendations or predictions that it makes;

(c) the mitigation measures established under section 8 in respect of it; and

(d) any other information that may be prescribed by regulation.

### **Notification of material harm**

12 A person who is responsible for a high-impact system must, in accordance with the regulations and as soon as feasible, notify the Minister if the use of the system results or is likely to result in material harm.

### **Ministerial Orders**

#### **Provision of subsection 10(1) records**

13 The Minister may, by order, require that a person referred to in subsection 10(1) provide the Minister with any of the records referred to in that subsection.

#### **Provision of subsection 10(2) records**

14 If the Minister has reasonable grounds to believe that the use of a high-impact system could result in harm or biased output, the Minister may, by order, require that a person referred to in subsection 10(2) provide the Minister, in the form specified in the order, with any of the records referred to in that subsection that relate to that system.

### **Audit**

15 (1) If the Minister has reasonable grounds to believe that a person has contravened any of sections 6 to 12 or an order made under section 13 or 14, the Minister may, by order, require that the person

(a) conduct an audit with respect to the possible contravention; or

(b) engage the services of an independent auditor to conduct the audit.

### **Qualifications**

(2) The audit must be conducted by a person who meets the qualifications that are prescribed by regulation.

### **Assistance**



(3) If the audit is conducted by an independent auditor, the person who is audited must give all assistance that is reasonably required to enable the auditor to conduct the audit, including by providing any records or other information specified by the auditor.

### **Report**

(4) The person who is audited must provide the Minister with the audit report.

### **Cost**

(5) In all cases, the cost of the audit is payable by the person who is audited.

### **Implementation of measures**

16 The Minister may, by order, require that a person who has been audited implement any measure specified in the order to address anything referred to in the audit report.

### **Cessation**

17 (1) The Minister may, by order, require that any person who is responsible for a high-impact system cease using it or making it available for use if the Minister has reasonable grounds to believe that the use of the system gives rise to a serious risk of imminent harm.

### **Statutory Instruments Act**

(2) The order is exempt from the application of sections 3 and 9 of the *Statutory Instruments Act*.

### **Publication**

18 (1) The Minister may, by order, require that a person referred to in any of sections 6 to 12, 15 and 16 publish, on a publicly available website, any information related to any of those sections. However, the Minister is not permitted to require that the person disclose confidential business information.

### **Regulations**

(2) The person must publish the information under subsection (1) in accordance with any regulations.

### **Compliance**

19 A person who is the subject of an order made by the Minister under this Part must comply with the order.

### **Filing — Federal Court**

20 The Minister may file a certified copy of an order made under any of sections 13 to 18 in the Federal Court and, on the certified copy being filed, the order becomes and may be enforced as an order of the Federal Court.

### **Statutory Instruments Act**

21 An order made under any of sections 13 to 16 and 18 is not a *statutory instrument* as defined in subsection 2(1) of the *Statutory Instruments Act*.

### Information

#### **Confidential nature maintained**

22 For greater certainty, confidential business information that is obtained by the Minister under this Part does not lose its confidential nature by the mere fact that it is so obtained or that it has been disclosed by the Minister under section 25 or 26.

#### **Obligation of Minister**

23 Subject to sections 24 to 26, the Minister must take measures to maintain the confidentiality of any confidential business information that the Minister obtains under this Part.

#### **Disclosure of confidential business information — subpoena, warrant, etc.**

24 The Minister may disclose confidential business information for the purpose of complying with a subpoena or warrant issued or order made by a court, person or body with jurisdiction to compel the production of information or for the purpose of complying with rules of court relating to the production of information.

#### **Disclosure of information — analyst**

25 (1) The Minister may disclose any information that is obtained under this Part to an analyst designated under section 34.

#### **Conditions — confidentiality**

(2) The Minister may impose any condition on the analyst in order to protect the confidentiality of information that the Minister discloses.

#### **Duty and restriction**

(3) An analyst must maintain the confidentiality of information disclosed to them under subsection (1) and may use the information only for the administration and enforcement of this Part.

#### **Disclosure of information — others**

26 (1) The Minister may disclose any information obtained under this Part to any of the following recipients, if the Minister has reasonable grounds to believe that a person who carries out any

regulated activity has contravened, or is likely to contravene, another Act of Parliament or a provincial legislature that is administered or enforced by the intended recipient of the information and if the information is relevant to the intended recipient's powers, duties or functions under that Act:

(a) the Privacy Commissioner;

(b) the Canadian Human Rights Commission;

(c) the Commissioner of Competition;

(d) the Canadian Radio-television and Telecommunications Commission;

(e) any person appointed by the government of a province, or any provincial entity, with powers, duties and functions that are similar to those of the Privacy Commissioner or the Canadian Human Rights Commission;

(f) any other person or entity prescribed by regulation.

### **Restriction**

(2) The Minister may disclose personal information or confidential business information under subsection (1) only if

(a) the Minister is satisfied that the disclosure is necessary for the purposes of enabling the recipient to administer or enforce the Act in question; and

(b) the recipient agrees in writing to maintain the confidentiality of the information except as necessary for any of those purposes.

### **Restriction — use**

(3) The recipient may use the disclosed information only for the purpose of the administration and enforcement of the Act in question.

### **Publication of information — contravention**

27 (1) If the Minister considers that it is in the public interest to do so, the Minister may, for the purpose of encouraging compliance with this Part, publish information about any contravention of this Part on a publicly available website.

### **Restriction**

(2) However, the Minister is not permitted to publish confidential business information under subsection (1).

### **Publication of information — harm**

28 (1) Without the consent of the person to whom the information relates and without notifying that person, the Minister may publish, on a publicly available website, information that relates to an artificial intelligence system and that is obtained under this Part if the Minister has reasonable grounds to believe that

(a) the use of the system gives rise to a serious risk of imminent harm; and

(b) the publication of the information is essential to prevent the harm.

### **Restriction**

(2) However, the Minister is not permitted to publish personal information or confidential business information under subsection (1).

### **Administrative Monetary Penalties**

#### **Administrative monetary penalties**

29 (1) A person who is found under the regulations to have committed a violation is liable to the administrative monetary penalty established by the regulations.

#### **Purpose of penalty**

(2) The purpose of an administrative monetary penalty is to promote compliance with this Part and not to punish.

#### **Violation or offence**

(3) If an act or omission may be proceeded with as a violation or as an offence, proceeding with it in one manner precludes proceeding with it in the other.

### **Regulations**

(4) The Governor in Council may make regulations respecting an administrative monetary penalties scheme, including regulations

(a) designating the provisions of this Part or of the regulations the contravention of which constitutes a violation, including those provisions the contravention of which, if continued on more than one day, constitutes a separate violation in respect of each day during which the violation is continued;

(b) classifying each violation as a minor violation, a serious violation or a very serious violation;

(c) respecting the proceedings in respect of a violation, including in relation to

(i) commencing the proceedings,

- (ii) maintaining the confidentiality of confidential business information in the proceedings,
- (iii) the defences that may be available in respect of a violation, and
- (iv) the circumstances in which the proceedings may be brought to an end;
- (d) respecting the administrative monetary penalties that may be imposed for a violation, including in relation to
  - (i) the amount, or range of amounts, of the administrative monetary penalties that may be imposed on persons or classes of persons,
  - (ii) the factors to be taken into account in imposing an administrative monetary penalty,
  - (iii) the payment of administrative monetary penalties that have been imposed, and
  - (iv) the recovery, as a debt, of unpaid administrative monetary penalties;
- (e) respecting reviews or appeals of findings that a violation has been committed and of the imposition of administrative monetary penalties;
- (f) respecting compliance agreements; and
- (g) respecting the persons or classes of persons who may exercise any power, or perform any duty or function, in relation to the scheme, including the designation of such persons or classes of persons by the Minister.

#### Offences

#### **Contravention — sections 6 to 12**

**30 (1) Every person who contravenes any of sections 6 to 12 is guilty of an offence.**

#### **Obstruction or providing false or misleading information**

**(2) Every person who carries out a regulated activity is guilty of an offence if the person obstructs — or provides false or misleading information to — the Minister, anyone acting on behalf of the Minister or an independent auditor in the exercise of their powers or performance of their duties or functions under this Part.**

#### **Punishment**

**(3) A person who commits an offence under subsection (1) or (2)**

**(a) is liable, on conviction on indictment,**

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

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

(b) is liable, on summary conviction,

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

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

### **Defence of due diligence**

(4) A person is not to be found guilty of an offence under subsection (1) or (2) if they establish that they exercised due diligence to prevent the commission of the offence.

### **Employee, agent or mandatary**

(5) It is sufficient proof of an offence under subsection (1) or (2) to establish that it was committed by an employee, agent or mandatary of the accused, whether or not the employee, agent or mandatary is identified or has been prosecuted for the offence, unless the accused establishes that the offence was committed without the knowledge or consent of the accused.

### **Administration**

#### **Designation**

31 The Governor in Council may, by order, designate any member of the Queen's Privy Council for Canada to be the Minister for the purposes of this Part.

#### **General powers of Minister**

32 The Minister may

(a) promote public awareness of this Act and provide education with respect to it;

(b) make recommendations and cause to be prepared reports on the establishment of measures to facilitate compliance with this Part; and

(c) establish guidelines with respect to compliance with this Part.

#### **Artificial Intelligence and Data Commissioner**

33 (1) The Minister may designate a senior official of the department over which the Minister presides to be called the Artificial Intelligence and Data Commissioner, whose role is to assist the Minister in the administration and enforcement of this Part.

### Delegation

(2) The Minister may delegate to the Commissioner any power, duty or function conferred on the Minister under this Part, except the power to make regulations under section 37.

### Analysts

34 The Minister may designate any individual or class of individuals as analysts for the administration and enforcement of this Part.

### Advisory committee

35 (1) The Minister may establish a committee to provide the Minister with advice on any matters related to this Part.

### Advice available to public

(2) The Minister may cause the advice that the committee provides to the Minister to be published on a publicly available website.

### Remuneration and expenses

(3) Each committee member is to be paid the remuneration fixed by the Governor in Council and is entitled to the reasonable travel and living expenses that they incur while performing their duties away from their ordinary place of residence.

### Regulations — Governor in Council

36 The Governor in Council may make regulations for the purposes of this Part, including regulations

(a) respecting what constitutes or does not constitute justification for the purpose of the definition *biased output* in subsection 5(1);

(b) establishing criteria for the purpose of the definition *high-impact system* in subsection 5(1);

(c) respecting the establishment of measures for the purposes of sections 6, 8 and 9;

(d) respecting the assessment for the purposes of section 7;

(e) respecting what constitutes or does not constitute material harm for the purpose of section 12;

(f) prescribing qualifications for the purposes of subsection 15(2); and

(g) prescribing persons and entities for the purpose of paragraph 26(1)(f).

### Regulations — Minister

37 The Minister may make regulations

- (a) respecting the records required to be kept under section 10;
- (b) prescribing, for the purposes of subsections 11(1) and (2), the time and the manner in which descriptions are to be published and the information to be included in the descriptions;
- (c) respecting the notice required to be provided under section 12; and
- (d) respecting the publication of information under section 18.

**PART 2**

**General Offences Related to Artificial Intelligence Systems**

**Possession or use of personal information**

38 Every person commits an offence if, for the purpose of designing, developing, using or making available for use an artificial intelligence system, the person possesses — within the meaning of subsection 4(3) of the *Criminal Code* — or uses personal information, knowing or believing that the information is obtained or derived, directly or indirectly, as a result of

- (a) the commission in Canada of an offence under an Act of Parliament or a provincial legislature; or
- (b) an act or omission anywhere that, if it had occurred in Canada, would have constituted such an offence.

**Making system available for use**

39 Every person commits an offence if the person

- (a) without lawful excuse and knowing that or being reckless as to whether the use of an artificial intelligence system is likely to cause serious physical or psychological harm to an individual or substantial damage to an individual's property, makes the artificial intelligence system available for use and the use of the system causes such harm or damage; or
- (b) with intent to defraud the public and to cause substantial economic loss to an individual, makes an artificial intelligence system available for use and its use causes that loss.

**Punishment**

40 Every person who commits an offence under section 38 or 39

- (a) is liable, on conviction on indictment,
  - (i) to a fine of not more than the greater of \$25,000,000 and 5% of the person's gross global revenues in its financial year before the one in which the person is sentenced, in the case of a person who is not an individual, and



(ii) to a fine in the discretion of the court or to a term of imprisonment of up to five years less a day, or to both, in the case of an individual; or

(b) is liable, on summary conviction,

(i) to a fine of not more than the greater of \$20,000,000 and 4% of the person's gross global revenues in its financial year before the one in which the person is sentenced, in the case of a person who is not an individual, and

(ii) to a fine of not more than \$100,000 or to a term of imprisonment of up to two years less a day, or to both, in the case of an individual.

### **PART 3),**

#### **Coming into Force**

#### **Order in council**

41 The provisions of this Act come into force on a day or days to be fixed by order of the Governor in Council.

### **PART 4**

#### **Coming into Force**

#### **Order in council**

**40 This Act, other than ~~section 34~~sections 2, 35, 36 and 39, comes into force on a day to be fixed by order of the Governor in Council.**

#### **Order in council**

~~(2) Sections 72 and 120 of the Consumer Privacy Protection Act, enacted by section 2 of this Act, come into force on a day to be fixed by order of the Governor in Council.~~

#### **Order in council**

~~(3) Sections 76 to 81, paragraph 83(1)(d), subsection 93(3) and section 122 of the Consumer Privacy Protection Act, enacted by section 2 of this Act, come into force on a day to be fixed by order of the Governor in Council.~~

**SCHEDULE**

(Section 2)

**SCHEDULE**

(Subsection 6(3) and paragraph ~~119(2)~~[122\(2\)](#)(c))

[Organizations](#)

<b>Organizations</b>		
Item	Column 1 Organization	Column 2 Personal Information
1	World Anti-Doping Agency	Personal information that the organization collects, uses or discloses in the course of its interprovincial or international activities

## EXPLANATORY NOTES

### Personal Information Protection and Electronic Documents Act

*Clause 3:* Existing text of the long title:

An Act to support and promote electronic commerce by protecting personal information that is collected, used or disclosed in certain circumstances, by providing for the use of electronic means to communicate or record information or transactions and by amending the Canada Evidence Act, the Statutory Instruments Act and the Statute Revision Act

*Clause 4:* Existing text of sections 1 to 30:

**1** This Act may be cited as the *Personal Information Protection and Electronic Documents Act*.

## PART 1

### Protection of Personal Information in the Private Sector

#### Interpretation

**2 (1)** The definitions in this subsection apply in this Part.

*alternative format*, with respect to personal information, means a format that allows a person with a sensory disability to read or listen to the personal information.

*breach of security safeguards* means the loss of, unauthorized access to or unauthorized disclosure of personal information resulting from a breach of an organization's security safeguards that are referred to in clause 4.7 of Schedule 1 or from a failure to establish those safeguards.

*business contact information* means any information that is used for the purpose of communicating or facilitating communication with an individual in relation to their employment, business or profession such as the individual's name, position name or title, work address, work telephone number, work fax number or work electronic address.

*business transaction* includes

- (a) the purchase, sale or other acquisition or disposition of an organization or a part of an organization, or any of its assets;
- (b) the merger or amalgamation of two or more organizations;
- (c) the making of a loan or provision of other financing to an organization or a part of an organization;
- (d) the creating of a charge on, or the taking of a security interest in or a security on, any assets or securities of an organization;

- (e) the lease or licensing of any of an organization's assets; and
- (f) any other prescribed arrangement between two or more organizations to conduct a business activity.

**commercial activity** means any particular transaction, act or conduct or any regular course of conduct that is of a commercial character, including the selling, bartering or leasing of donor, membership or other fundraising lists.

**Commissioner** means the Privacy Commissioner appointed under section 53 of the *Privacy Act*.

**Court** means the Federal Court.

**federal work, undertaking or business** means any work, undertaking or business that is within the legislative authority of Parliament. It includes

- (a) a work, undertaking or business that is operated or carried on for or in connection with navigation and shipping, whether inland or maritime, including the operation of ships and transportation by ship anywhere in Canada;
- (b) a railway, canal, telegraph or other work or undertaking that connects a province with another province, or that extends beyond the limits of a province;
- (c) a line of ships that connects a province with another province, or that extends beyond the limits of a province;
- (d) a ferry between a province and another province or between a province and a country other than Canada;
- (e) aerodromes, aircraft or a line of air transportation;
- (f) a radio broadcasting station;
- (g) a bank or an authorized foreign bank as defined in section 2 of the *Bank Act*;
- (h) a work that, although wholly situated within a province, is before or after its execution declared by Parliament to be for the general advantage of Canada or for the advantage of two or more provinces;
- (i) a work, undertaking or business outside the exclusive legislative authority of the legislatures of the provinces; and
- (j) a work, undertaking or business to which federal laws, within the meaning of section 2 of the *Oceans Act*, apply under section 20 of that Act and any regulations made under paragraph 26(1)(k) of that Act.

**organization** includes an association, a partnership, a person and a trade union.

**personal health information**, with respect to an individual, whether living or deceased, means

- (a) information concerning the physical or mental health of the individual;
- (b) information concerning any health service provided to the individual;
- (c) information concerning the donation by the individual of any body part or any bodily substance of the individual or information derived from the testing or examination of a body part or bodily substance of the individual;
- (d) information that is collected in the course of providing health services to the individual; or
- (e) information that is collected incidentally to the provision of health services to the individual.

*personal information* means information about an identifiable individual.

*prescribed* means prescribed by regulation.

*record* includes any correspondence, memorandum, book, plan, map, drawing, diagram, pictorial or graphic work, photograph, film, microform, sound recording, videotape, machine-readable record and any other documentary material, regardless of physical form or characteristics, and any copy of any of those things.

(2) In this Part, a reference to clause 4.3 or 4.9 of Schedule 1 does not include a reference to the note that accompanies that clause.

#### Purpose

3 The purpose of this Part is to establish, in an era in which technology increasingly facilitates the circulation and exchange of information, rules to govern the collection, use and disclosure of personal information in a manner that recognizes the right of privacy of individuals with respect to their personal information and the need of organizations to collect, use or disclose personal information for purposes that a reasonable person would consider appropriate in the circumstances.

#### Application

4 (1) This Part applies to every organization in respect of personal information that

- (a) the organization collects, uses or discloses in the course of commercial activities; or
- (b) is about an employee of, or an applicant for employment with, the organization and that the organization collects, uses or discloses in connection with the operation of a federal work, undertaking or business.

(1.1) This Part applies to an organization set out in column 1 of Schedule 4 in respect of personal information set out in column 2.

(2) This Part does not apply to

- (a) any government institution to which the *Privacy Act* applies;
- (b) any individual in respect of personal information that the individual collects, uses or discloses for personal or domestic purposes and does not collect, use or disclose for any other purpose; or
- (c) any organization in respect of personal information that the organization collects, uses or discloses for journalistic, artistic or literary purposes and does not collect, use or disclose for any other purpose.

\*(3) Every provision of this Part applies despite any provision, enacted after this subsection comes into force, of any other Act of Parliament, unless the other Act expressly declares that that provision operates despite the provision of this Part.

\* [Note: Subsection 4(3) in force January 1, 2001, *see* SI/ 2000-29.]

**4.01** This Part does not apply to an organization in respect of the business contact information of an individual that the organization collects, uses or discloses solely for the purpose of communicating or facilitating communication with the individual in relation to their employment, business or profession.

**4.1 (1)** Where a certificate under section 38.13 of the *Canada Evidence Act* prohibiting the disclosure of personal information of a specific individual is issued before a complaint is filed by that individual under this Part in respect of a request for access to that information, the provisions of this Part respecting that individual's right of access to his or her personal information do not apply to the information that is subject to the certificate.

(2) Notwithstanding any other provision of this Part, where a certificate under section 38.13 of the *Canada Evidence Act* prohibiting the disclosure of personal information of a specific individual is issued after the filing of a complaint under this Part in relation to a request for access to that information:

- (a) all proceedings under this Part in respect of that information, including an investigation, audit, appeal or judicial review, are discontinued;
- (b) the Commissioner shall not disclose the information and shall take all necessary precautions to prevent its disclosure; and
- (c) the Commissioner shall, within 10 days after the certificate is published in the *Canada Gazette*, return the information to the organization that provided the information.

(3) The Commissioner and every person acting on behalf or under the direction of the Commissioner, in carrying out their functions under this Part, shall not disclose information subject to a certificate issued under section 38.13 of the *Canada Evidence Act*, and shall take every reasonable precaution to avoid the disclosure of that information.

(4) The Commissioner may not delegate the investigation of any complaint relating to information subject to a certificate issued under section 38.13 of the *Canada Evidence Act* except to one of a maximum of four officers or employees of the Commissioner specifically designated by the Commissioner for the purpose of conducting that investigation.

## **DIVISION 1**

### Protection of Personal Information

**5 (1)** Subject to sections 6 to 9, every organization shall comply with the obligations set out in Schedule 1.

(2) The word *should*, when used in Schedule 1, indicates a recommendation and does not impose an obligation.

(3) An organization may collect, use or disclose personal information only for purposes that a reasonable person would consider are appropriate in the circumstances.

**6** The designation of an individual under clause 4.1 of Schedule 1 does not relieve the organization of the obligation to comply with the obligations set out in that Schedule.

**6.1** For the purposes of clause 4.3 of Schedule 1, the consent of an individual 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.

**7 (1)** For the purpose of clause 4.3 of Schedule 1, and despite the note that accompanies that clause, an organization may collect personal information without the knowledge or consent of the individual only if

(a) the collection is clearly in the interests of the individual and consent cannot be obtained in a timely way;

(b) it is reasonable to expect that the collection with the knowledge or consent of the individual would compromise the availability or the accuracy of the information and the collection is reasonable for purposes related to investigating a breach of an agreement or a contravention of the laws of Canada or a province;

(b.1) it is contained in a witness statement and the collection is necessary to assess, process or settle an insurance claim;

(b.2) it was produced by the individual in the course of their employment, business or profession and the collection is consistent with the purposes for which the information was produced;

(c) the collection is solely for journalistic, artistic or literary purposes;

(d) the information is publicly available and is specified by the regulations; or

(e) the collection is made for the purpose of making a disclosure

(i) under subparagraph (3)(c.1)(i) or (d)(ii), or

(ii) that is required by law.

(2) For the purpose of clause 4.3 of Schedule 1, and despite the note that accompanies that clause, an organization may, without the knowledge or consent of the individual, use personal information only if

(a) in the course of its activities, the organization becomes aware of information that it has reasonable grounds to believe could be useful in the investigation of a contravention of the laws of Canada, a province or a foreign jurisdiction that has been, is being or is about to be committed, and the information is used for the purpose of investigating that contravention;

(b) it is used for the purpose of acting in respect of an emergency that threatens the life, health or security of an individual;

(b.1) the information is contained in a witness statement and the use is necessary to assess, process or settle an insurance claim;

(b.2) the information was produced by the individual in the course of their employment, business or profession and the use is consistent with the purposes for which the information was produced;

(c) 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;

(c.1) it is publicly available and is specified by the regulations; or

(d) it was collected under paragraph (1)(a), (b) or (e).

(3) For the purpose of clause 4.3 of Schedule 1, and despite the note that accompanies that clause, an organization may disclose personal information without the knowledge or consent of the individual only if the disclosure is

(a) made to, in the Province of Quebec, an advocate or notary or, in any other province, a barrister or solicitor who is representing the organization;

(b) for the purpose of collecting a debt owed by the individual to the organization;

(c) required to comply with a subpoena or warrant issued or an order made by a court, person or body with jurisdiction to compel the production of information, or to comply with rules of court relating to the production of records;



**(c.1)** made to a government institution or part of a government institution that has made a request for the information, identified its lawful authority to obtain the information and indicated that

**(i)** it suspects that the information relates to national security, the defence of Canada or the conduct of international affairs,

**(ii)** the disclosure is requested for the purpose of enforcing any law of Canada, a province or a foreign jurisdiction, carrying out an investigation relating to the enforcement of any such law or gathering intelligence for the purpose of enforcing any such law,

**(iii)** the disclosure is requested for the purpose of administering any law of Canada or a province, or

**(iv)** the disclosure is requested for the purpose of communicating with the next of kin or authorized representative of an injured, ill or deceased individual;

**(c.2)** made to the government institution mentioned in section 7 of the *Proceeds of Crime (Money Laundering) and Terrorist Financing Act* as required by that section;

**(d)** made on the initiative of the organization to a government institution or a part of a government institution and the organization

**(i)** has reasonable grounds to believe that the information relates to a contravention of the laws of Canada, a province or a foreign jurisdiction that has been, is being or is about to be committed, or

**(ii)** suspects that the information relates to national security, the defence of Canada or the conduct of international affairs;

**(d.1)** made to another organization and is reasonable for the purposes of investigating a breach of an agreement or a contravention of the laws of Canada or a province that has been, is being or is about to be committed and it is reasonable to expect that disclosure with the knowledge or consent of the individual would compromise the investigation;

**(d.2)** made to another organization and is reasonable for the purposes of detecting or suppressing fraud or of preventing fraud that is likely to be committed and it is reasonable to expect that the disclosure with the knowledge or consent of the individual would compromise the ability to prevent, detect or suppress the fraud;

**(d.3)** made on the initiative of the organization to a government institution, a part of a government institution or the individual's next of kin or authorized representative and

**(i)** the organization has reasonable grounds to believe that the individual has been, is or may be the victim of financial abuse,

**(ii)** the disclosure is made solely for purposes related to preventing or investigating the abuse, and

(iii) it is reasonable to expect that disclosure with the knowledge or consent of the individual would compromise the ability to prevent or investigate the abuse;

(d.4) necessary to identify the individual who is injured, ill or deceased, made to a government institution, a part of a government institution or the individual's next of kin or authorized representative and, if the individual is alive, the organization informs that individual in writing without delay of the disclosure;

(e) made to a person who needs the information because of an emergency that threatens the life, health or security of an individual and, if the individual whom the information is about is alive, ~~he~~the organization informs that individual in writing without delay of the disclosure;

(e.1) of information that is contained in a witness statement and the disclosure is necessary to assess, process or settle an insurance claim;

(e.2) of information that was produced by the individual in the course of their employment, business or profession and the disclosure is consistent with the purposes for which the information was produced;

(f) for statistical, or scholarly study or research, purposes that cannot be achieved without disclosing the information, it is impracticable to obtain consent and the organization informs the Commissioner of the disclosure before the information is disclosed;

(g) made to an institution whose functions include the conservation of records of historic or archival importance, and the disclosure is made for the purpose of such conservation;

(h) made after the earlier of

(i) one hundred years after the record containing the information was created, and

(ii) twenty years after the death of the individual whom the information is about;

(h.1) of information that is publicly available and is specified by the regulations; or

(h.2) [Repealed, 2015, c. 32, s. 6]

(i) required by law.

(4) Despite clause 4.5 of Schedule 1, an organization may use personal information for purposes other than those for which it was collected in any of the circumstances set out in subsection (2).

(5) Despite clause 4.5 of Schedule 1, an organization may disclose personal information for purposes other than those for which it was collected in any of the circumstances set out in paragraphs (3)(a) to (h.1).

**7.1 (1)** The following definitions apply in this section.

**access** means to program, to execute programs on, to communicate with, to store data in, to retrieve data from, or to otherwise make use of any resources, including data or programs on a computer system or a computer network.

**computer program** has the same meaning as in subsection 342.1(2) of the *Criminal Code*.

**computer system** has the same meaning as in subsection 342.1(2) of the *Criminal Code*.

**electronic address** means an address used in connection with

- (a) an electronic mail account;
- (b) an instant messaging account; or
- (c) any similar account.

**(2)** Paragraphs 7(1)(a) and (b.1) to (d) and (2)(a) to (c.1) and the exception set out in clause 4.3 of Schedule 1 do not apply in respect of

- (a) the collection of an individual's electronic address, if the address is collected by the use of a computer program that is designed or marketed primarily for use in generating or searching for, and collecting, electronic addresses; or
- (b) the use of an individual's electronic address, if the address is collected by the use of a computer program described in paragraph (a).

**(3)** Paragraphs 7(1)(a) to (d) and (2)(a) to (c.1) and the exception set out in clause 4.3 of Schedule 1 do not apply in respect of

- (a) the collection of personal information, through any means of telecommunication, if the collection is made by accessing a computer system or causing a computer system to be accessed in contravention of an Act of Parliament; or
- (b) the use of personal information that is collected in a manner described in paragraph (a).

**7.2 (1)** In addition to the circumstances set out in subsections 7(2) and (3), for the purpose of clause 4.3 of Schedule 1, and despite the note that accompanies that clause, organizations that are parties to a prospective business transaction may use and disclose personal information without the knowledge or consent of the individual if

- (a) the organizations have entered into an agreement that requires the organization that receives the personal information
  - (i) to use and disclose that information solely for purposes related to the transaction,
  - (ii) to protect that information by security safeguards appropriate to the sensitivity of the information, and

(iii) if the transaction does not proceed, to return that information to the organization that disclosed it, or destroy it, within a reasonable time; and

(b) the personal information is necessary

(i) to determine whether to proceed with the transaction, and

(ii) if the determination is made to proceed with the transaction, to complete it.

(2) In addition to the circumstances set out in subsections 7(2) and (3), for the purpose of clause 4.3 of Schedule 1, and despite the note that accompanies that clause, if the business transaction is completed, organizations that are parties to the transaction may use and disclose personal information, which was disclosed under subsection (1), without the knowledge or consent of the individual if

(a) the organizations have entered into an agreement that requires each of them

(i) to use and disclose the personal information under its control solely for the purposes for which the personal information was collected, permitted to be used or disclosed before the transaction was completed,

(ii) to protect that information by security safeguards appropriate to the sensitivity of the information, and

(iii) to give effect to any withdrawal of consent made under clause 4.3.8 of Schedule 1;

(b) the personal information is necessary for carrying on the business or activity that was the object of the transaction; and

(c) one of the parties notifies the individual, within a reasonable time after the transaction is completed, that the transaction has been completed and that their personal information has been disclosed under subsection (1).

(3) An organization shall comply with the terms of any agreement into which it enters under paragraph (1)(a) or (2)(a).

(4) Subsections (1) and (2) do not apply to a business transaction of which the primary purpose or result is the purchase, sale or other acquisition or disposition, or lease, of personal information.

**7.3** In addition to the circumstances set out in section 7, for the purpose of clause 4.3 of Schedule 1, and despite the note that accompanies that clause, a federal work, undertaking or business may collect, use and disclose personal information without the consent of the individual if

(a) the collection, use or disclosure is necessary to establish, manage or terminate an employment relationship between the federal work, undertaking or business and the individual; and

(b) the federal work, undertaking or business has informed the individual that the personal information will be or may be collected, used or disclosed for those purposes.

**7.4 (1)** Despite clause 4.5 of Schedule 1, an organization may use personal information for purposes other than those for which it was collected in any of the circumstances set out in subsection 7.2(1) or (2) or section 7.3.

(2) Despite clause 4.5 of Schedule 1, an organization may disclose personal information for purposes other than those for which it was collected in any of the circumstances set out in subsection 7.2(1) or (2) or section 7.3.

**8 (1)** A request under clause 4.9 of Schedule 1 must be made in writing.

(2) An organization shall assist any individual who informs the organization that they need assistance in preparing a request to the organization.

(3) An organization shall respond to a request with due diligence and in any case not later than thirty days after receipt of the request.

(4) An organization may extend the time limit

(a) for a maximum of thirty days if

(i) meeting the time limit would unreasonably interfere with the activities of the organization, or

(ii) the time required to undertake any consultations necessary to respond to the request would make the time limit impracticable to meet; or

(b) for the period that is necessary in order to be able to convert the personal information into an alternative format.

In either case, the organization shall, no later than thirty days after the date of the request, send a notice of extension to the individual, advising them of the new time limit, the reasons for extending the time limit and of their right to make a complaint to the Commissioner in respect of the extension.

(5) If the organization fails to respond within the time limit, the organization is deemed to have refused the request.

(6) An organization may respond to an individual's request at a cost to the individual only if

(a) the organization has informed the individual of the approximate cost; and

(b) the individual has advised the organization that the request is not being withdrawn.

(7) An organization that responds within the time limit and refuses a request shall inform the individual in writing of the refusal, setting out the reasons and any recourse that they may have under this Part.

**(8)** Despite clause 4.5 of Schedule 1, an organization that has personal information that is the subject of a request shall retain the information for as long as is necessary to allow the individual to exhaust any recourse under this Part that they may have.

**9 (1)** Despite clause 4.9 of Schedule 1, an organization shall not give an individual access to personal information if doing so would likely reveal personal information about a third party. However, if the information about the third party is severable from the record containing the information about the individual, the organization shall sever the information about the third party before giving the individual access.

**(2)** Subsection (1) does not apply if the third party consents to the access or the individual needs the information because an individual's life, health or security is threatened.

**(2.1)** An organization shall comply with subsection (2.2) if an individual requests that the organization

**(a)** inform the individual about

**(i)** any disclosure of information to a government institution or a part of a government institution under paragraph 7(3)(c), subparagraph 7(3)(c.1)(i) or (ii) or paragraph 7(3)(c.2) or (d), or

**(ii)** the existence of any information that the organization has relating to a disclosure referred to in subparagraph (i), to a subpoena, warrant or order referred to in paragraph 7(3)(c) or to a request made by a government institution or a part of a government institution under subparagraph 7(3)(c.1)(i) or (ii); or

**(b)** give the individual access to the information referred to in subparagraph (a)(ii).

**(2.2)** An organization to which subsection (2.1) applies

**(a)** shall, in writing and without delay, notify the institution or part concerned of the request made by the individual; and

**(b)** shall not respond to the request before the earlier of

**(i)** the day on which it is notified under subsection (2.3), and

**(ii)** thirty days after the day on which the institution or part was notified.

**(2.3)** Within thirty days after the day on which it is notified under subsection (2.2), the institution or part shall notify the organization whether or not the institution or part objects to the organization complying with the request. The institution or part may object only if the institution or part is of the opinion that compliance with the request could reasonably be expected to be injurious to

**(a)** national security, the defence of Canada or the conduct of international affairs;

**(a.1)** the detection, prevention or deterrence of money laundering or the financing of terrorist activities; or

**(b)** the enforcement of any law of Canada, a province or a foreign jurisdiction, an investigation relating to the enforcement of any such law or the gathering of intelligence for the purpose of enforcing any such law.

**(2.4)** Despite clause 4.9 of Schedule 1, if an organization is notified under subsection (2.3) that the institution or part objects to the organization complying with the request, the organization

**(a)** shall refuse the request to the extent that it relates to paragraph (2.1)(a) or to information referred to in subparagraph (2.1)(a)(ii);

**(b)** shall notify the Commissioner, in writing and without delay, of the refusal; and

**(c)** shall not disclose to the individual

**(i)** any information that the organization has relating to a disclosure to a government institution or a part of a government institution under paragraph 7(3)(c), subparagraph 7(3)(c.1)(i) or (ii) or paragraph 7(3)(c.2) or (d) or to a request made by a government institution under either of those subparagraphs,

**(ii)** that the organization notified an institution or part under paragraph (2.2)(a) or the Commissioner under paragraph (b), or

**(iii)** that the institution or part objects.

**(3)** Despite the note that accompanies clause 4.9 of Schedule 1, an organization is not required to give access to personal information only if

**(a)** the information is protected by solicitor-client privilege or the professional secrecy of advocates and notaries or by litigation privilege;

**(b)** to do so would reveal confidential commercial information;

**(c)** to do so could reasonably be expected to threaten the life or security of another individual;

**(c.1)** the information was collected under paragraph 7(1)(b);

**(d)** the information was generated in the course of a formal dispute resolution process; or

**(e)** the information was created for the purpose of making a disclosure under the *Public Servants Disclosure Protection Act* or in the course of an investigation into a disclosure under that Act.

However, in the circumstances described in paragraph (b) or (c), if giving access to the information would reveal confidential commercial information or could reasonably be expected to threaten the life or security of another individual, as the case may be, and that information is severable from the

record containing any other information for which access is requested, the organization shall give the individual access after severing.

(4) Subsection (3) does not apply if the individual needs the information because an individual's life, health or security is threatened.

(5) If an organization decides not to give access to personal information in the circumstances set out in paragraph (3)(c.1), the organization shall, in writing, so notify the Commissioner, and shall include in the notification any information that the Commissioner may specify.

**10** An organization shall give access to personal information in an alternative format to an individual with a sensory disability who has a right of access to personal information under this Part and who requests that it be transmitted in the alternative format if

(a) a version of the information already exists in that format; or

(b) its conversion into that format is reasonable and necessary in order for the individual to be able to exercise rights under this Part.

## **DIVISION 1.1**

### Breaches of Security Safeguards

**10.1 (1)** An organization shall report to the Commissioner any breach of security safeguards involving personal information under its control if it is reasonable in the circumstances to believe that the breach creates a real risk of significant harm to an individual.

(2) The report shall contain the prescribed information and shall be made in the prescribed form and manner as soon as feasible after the organization determines that the breach has occurred.

(3) Unless otherwise prohibited by law, an organization shall notify an individual of any breach of security safeguards involving the individual's personal information under the organization's control if it is reasonable in the circumstances to believe that the breach creates a real risk of significant harm to the individual.

(4) The notification shall contain sufficient information to allow the individual to understand the significance to them of the breach and to take steps, if any are possible, to reduce the risk of harm that could result from it or to mitigate that harm. It shall also contain any other prescribed information.

(5) The notification shall be conspicuous and shall be given directly to the individual in the prescribed form and manner, except in prescribed circumstances, in which case it shall be given indirectly in the prescribed form and manner.

(6) The notification shall be given as soon as feasible after the organization determines that the breach has occurred.



(7) For the purpose of this section, *significant harm* includes bodily harm, humiliation, damage to reputation or relationships, loss of employment, business or professional opportunities, financial loss, identity theft, negative effects on the credit record and damage to or loss of property.

(8) The factors that are relevant to determining whether a breach of security safeguards creates a real risk of significant harm to the individual include

- (a) the sensitivity of the personal information involved in the breach;
- (b) the probability that the personal information has been, is being or will be misused; and
- (c) any other prescribed factor.

**10.2 (1)** An organization that notifies an individual of a breach of security safeguards under subsection 10.1(3) shall notify any other organization, a government institution or a part of a government institution of the breach if the notifying organization believes that the other organization or the government institution or part concerned may be able to reduce the risk of harm that could result from it or mitigate that harm, or if any of the prescribed conditions are satisfied.

(2) The notification shall be given as soon as feasible after the organization determines that the breach has occurred.

(3) In addition to the circumstances set out in subsection 7(3), for the purpose of clause 4.3 of Schedule 1, and despite the note that accompanies that clause, an organization may disclose personal information without the knowledge or consent of the individual if

- (a) the disclosure is made to the other organization, the government institution or the part of a government institution that was notified of the breach under subsection (1); and
- (b) the disclosure is made solely for the purposes of reducing the risk of harm to the individual that could result from the breach or mitigating that harm.

(4) Despite clause 4.5 of Schedule 1, an organization may disclose personal information for purposes other than those for which it was collected in the circumstance set out in subsection (3).

**10.3 (1)** An organization shall, in accordance with any prescribed requirements, keep and maintain a record of every breach of security safeguards involving personal information under its control.

(2) An organization shall, on request, provide the Commissioner with access to, or a copy of, a record.

## **DIVISION 2**

### Remedies

### **Filing of Complaints**

**11 (1)** An individual may file with the Commissioner a written complaint against an organization for contravening a provision of Division 1 or 1.1 or for not following a recommendation set out in Schedule 1.

**(2)** If the Commissioner is satisfied that there are reasonable grounds to investigate a matter under this Part, the Commissioner may initiate a complaint in respect of the matter.

**(3)** A complaint that results from the refusal to grant a request under section 8 must be filed within six months, or any longer period that the Commissioner allows, after the refusal or after the expiry of the time limit for responding to the request, as the case may be.

**(4)** The Commissioner shall give notice of a complaint to the organization against which the complaint was made.

### **Investigations of Complaints**

**12 (1)** The Commissioner shall conduct an investigation in respect of a complaint, unless the Commissioner is of the opinion that

**(a)** the complainant ought first to exhaust grievance or review procedures otherwise reasonably available;

**(b)** the complaint could more appropriately be dealt with, initially or completely, by means of a procedure provided for under the laws of Canada, other than this Part, or the laws of a province; or

**(c)** the complaint was not filed within a reasonable period after the day on which the subject matter of the complaint arose.

**(2)** Despite subsection (1), the Commissioner is not required to conduct an investigation in respect of an act alleged 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.

**(3)** The Commissioner shall notify the complainant and the organization that the Commissioner will not investigate the complaint or any act alleged in the complaint and give reasons.

**(4)** The Commissioner may reconsider a decision not to investigate under subsection (1), if the Commissioner is satisfied that the complainant has established that there are compelling reasons to investigate.

**12.1 (1)** In the conduct of an investigation of a complaint, the Commissioner may

(a) summon and enforce the appearance of persons before the Commissioner and compel them to give oral or written evidence on oath and to produce any records and things that the Commissioner considers necessary to investigate the complaint, in the same manner and to the same extent as a superior court of record;

(b) administer oaths;

(c) receive and accept any evidence and other information, whether on oath, by affidavit or otherwise, that the Commissioner sees fit, whether or not it is or would be admissible in a court of law;

(d) at any reasonable time, enter any premises, other than a dwelling-house, occupied by an organization on satisfying any security requirements of the organization relating to the premises;

(e) converse in private with any person in any premises entered under paragraph (d) and otherwise carry out in those premises any inquiries that the Commissioner sees fit; and

(f) examine or obtain copies of or extracts from records found in any premises entered under paragraph (d) that contain any matter relevant to the investigation.

(2) The Commissioner may attempt to resolve complaints by means of dispute resolution mechanisms such as mediation and conciliation.

(3) The Commissioner may delegate any of the powers set out in subsection (1) or (2).

(4) The Commissioner or the delegate shall return to a person or an organization any record or thing that they produced under this section within 10 days after they make a request to the Commissioner or the delegate, but nothing precludes the Commissioner or the delegate from again requiring that the record or thing be produced.

(5) Any person to whom powers set out in subsection (1) are delegated shall be given a certificate of the delegation and the delegate shall produce the certificate, on request, to the person in charge of any premises to be entered under paragraph (1)(d).

### **Discontinuance of Investigation**

**12.2 (1)** The Commissioner may discontinue the investigation of a complaint if the Commissioner is of the opinion that

(a) there is insufficient evidence to pursue the investigation;

(b) the complaint is trivial, frivolous or vexatious or is made in bad faith;

(c) the organization has provided a fair and reasonable response to the complaint;

(c.1) the matter is the object of a compliance agreement entered into under subsection 17.1(1);

(d) the matter is already the object of an ongoing investigation under this Part;

- (e) the matter has already been the subject of a report by the Commissioner;
- (f) any of the circumstances mentioned in paragraph 12(1)(a), (b) or (c) apply; or
- (g) the matter is being or has already been addressed under a procedure referred to in paragraph 12(1)(a) or (b).

(2) The Commissioner may discontinue an investigation in respect of an act alleged 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.

(3) The Commissioner shall notify the complainant and the organization that the investigation has been discontinued and give reasons.

### **Commissioner's Report**

**13 (1)** The Commissioner shall, within one year after the day on which a complaint is filed or is initiated by the Commissioner, prepare a report that contains

- (a) the Commissioner's findings and recommendations;
- (b) any settlement that was reached by the parties;
- (c) if appropriate, a request that the organization give the Commissioner, within a specified time, notice of any action taken or proposed to be taken to implement the recommendations contained in the report or reasons why no such action has been or is proposed to be taken; and
- (d) the recourse, if any, that is available under section 14.

(2) [Repealed, 2010, c. 23, s. 84]

(3) The report shall be sent to the complainant and the organization without delay.

### **Hearing by Court**

**14 (1)** A complainant may, after receiving the Commissioner's report or being notified under subsection 12.2(3) that the investigation of the complaint has been discontinued, apply to the Court for a hearing in respect of any matter in respect of which the complaint was made, or that is referred to in the Commissioner's report, and that is referred to in clause 4.1.3, 4.2, 4.3.3, 4.4, 4.6, 4.7 or 4.8 of Schedule 1, in clause 4.3, 4.5 or 4.9 of that Schedule as modified or clarified by Division 1 or 1.1, in subsection 5(3) or 8(6) or (7), in section 10 or in Division 1.1.

(2) A complainant shall make an application within one year after the report or notification is sent or within any longer period that the Court may, either before or after the expiry of that year, allow.

(3) For greater certainty, subsections (1) and (2) apply in the same manner to complaints referred to in subsection 11(2) as to complaints referred to in subsection 11(1).

**15** The Commissioner may, in respect of a complaint that the Commissioner did not initiate,

(a) apply to the Court, within the time limited by section 14, for a hearing in respect of any matter described in that section, if the Commissioner has the consent of the complainant;

(b) appear before the Court on behalf of any complainant who has applied for a hearing under section 14; or

(c) with leave of the Court, appear as a party to any hearing applied for under section 14.

**16** The Court may, in addition to any other remedies it may give,

(a) order an organization to correct its practices in order to comply with Divisions 1 and 1.1;

(b) order an organization to publish a notice of any action taken or proposed to be taken to correct its practices, whether or not ordered to correct them under paragraph (a); and

(c) award damages to the complainant, including damages for any humiliation that the complainant has suffered.

**17 (1)** An application made under section 14 or 15 shall be heard and determined without delay and in a summary way unless the Court considers it inappropriate to do so.

(2) In any proceedings arising from an application made under section 14 or 15, the Court shall take every reasonable precaution, including, when appropriate, receiving representations ex parte and conducting hearings in camera, to avoid the disclosure by the Court or any person of any information or other material that the organization would be authorized to refuse to disclose if it were requested under clause 4.9 of Schedule 1.

### **Compliance Agreements**

**17.1 (1)** If 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 a provision of Division 1 or 1.1 or a failure to follow a recommendation set out in Schedule 1, the Commissioner may enter into a compliance agreement, aimed at ensuring compliance with this Part, with that organization.

(2) A compliance agreement may contain any terms that the Commissioner considers necessary to ensure compliance with this Part.

(3) When a compliance agreement is entered into, the Commissioner, in respect of any matter covered under the agreement,

- (a) shall not apply to the Court for a hearing under subsection 14(1) or paragraph 15(a); and
- (b) shall apply to the court for the suspension of any pending applications that were made by the Commissioner under those provisions.

(4) For greater certainty, a compliance agreement does not preclude

- (a) an individual from applying for a hearing under section 14; or
- (b) the prosecution of an offence under the Act.

**17.2 (1)** If the Commissioner is of the opinion that a compliance agreement has been complied with, the Commissioner shall provide written notice to that effect to the organization and withdraw any applications that were made under subsection 14(1) or paragraph 15(a) in respect of any matter covered under the agreement.

(2) If the Commissioner is of the opinion that an organization is not complying with the terms of a compliance agreement, the Commissioner shall notify the organization and may apply to the Court for

- (a) an order requiring the organization to comply with the terms of the agreement, in addition to any other remedies it may give; or
- (b) a hearing under subsection 14(1) or paragraph 15(a) or to reinstate proceedings that have been suspended as a result of an application made under paragraph 17.1(3)(b).

(3) Despite subsection 14(2), the application shall be made within one year after notification is sent or within any longer period that the Court may, either before or after the expiry of that year, allow.

### **DIVISION 3**

#### Audits

**18 (1)** The Commissioner may, on reasonable notice and at any reasonable time, audit the personal information management practices of an organization if the Commissioner has reasonable grounds to believe that the organization has contravened a provision of Division 1 or 1.1 or is not following a recommendation set out in Schedule 1, and for that purpose may

- (a) summon and enforce the appearance of persons before the Commissioner and compel them to give oral or written evidence on oath and to produce any records and things that the Commissioner considers necessary for the audit, in the same manner and to the same extent as a superior court of record;
- (b) administer oaths;
- (c) receive and accept any evidence and other information, whether on oath, by affidavit or otherwise, that the Commissioner sees fit, whether or not it is or would be admissible in a court of law;

(d) at any reasonable time, enter any premises, other than a dwelling-house, occupied by the organization on satisfying any security requirements of the organization relating to the premises;

(e) converse in private with any person in any premises entered under paragraph (d) and otherwise carry out in those premises any inquiries that the Commissioner sees fit; and

(f) examine or obtain copies of or extracts from records found in any premises entered under paragraph (d) that contain any matter relevant to the audit.

(2) The Commissioner may delegate any of the powers set out in subsection (1).

(3) The Commissioner or the delegate shall return to a person or an organization any record or thing they produced under this section within ten days after they make a request to the Commissioner or the delegate, but nothing precludes the Commissioner or the delegate from again requiring that the record or thing be produced.

(4) Any person to whom powers set out in subsection (1) are delegated shall be given a certificate of the delegation and the delegate shall produce the certificate, on request, to the person in charge of any premises to be entered under paragraph (1)(d).

**19 (1)** After an audit, the Commissioner shall provide the audited organization with a report that contains the findings of the audit and any recommendations that the Commissioner considers appropriate.

(2) The report may be included in a report made under section 25.

## **DIVISION 4**

### General

**20 (1)** Subject to subsections (2) to (7), 12(3), 12.2(3), 13(3), 19(1), 23(3) and 23.1(1) and section 25, the Commissioner or any person acting on behalf or under the direction of the Commissioner shall not disclose any information that comes to their knowledge as a result of the performance or exercise of any of the Commissioner's duties or powers under this Part other than those referred to in subsection 10.1(1) or 10.3(2).

**(1.1)** Subject to subsections (2) to (7), 12(3), 12.2(3), 13(3), 19(1), 23(3) and 23.1(1) and section 25, the Commissioner or any person acting on behalf or under the direction of the Commissioner shall not disclose any information contained in a report made under subsection 10.1(1) or in a record obtained under subsection 10.3(2).

(2) The Commissioner may, if the Commissioner considers that it is in the public interest to do so, make public any information that comes to his or her knowledge in the performance or exercise of any of his or her duties or powers under this Part.

(3) The Commissioner may disclose, or may authorize any person acting on behalf or under the direction of the Commissioner to disclose, information that in the Commissioner's opinion is necessary to

- (a) conduct an investigation or audit under this Part; or
- (b) establish the grounds for findings and recommendations contained in any report under this Part.

(4) The Commissioner may disclose, or may authorize any person acting on behalf or under the direction of the Commissioner to disclose, information in the course of

- (a) a prosecution for an offence under section 28;
- (b) a prosecution for an offence under section 132 of the *Criminal Code* (perjury) in respect of a statement made under this Part;
- (c) a hearing before the Court under this Part;
- (d) an appeal from a decision of the Court; or
- (e) a judicial review in relation to the performance or exercise of any of the Commissioner's duties or powers under this Part.

(5) The Commissioner may disclose to the Attorney General of Canada or of a province, as the case may be, information relating to the commission of an offence against any law of Canada or a province on the part of an officer or employee of an organization if, in the Commissioner's opinion, there is evidence of an offence.

(6) The Commissioner may disclose, or may authorize any person acting on behalf or under the direction of the Commissioner to disclose to a government institution or a part of a government institution, any information contained in a report made under subsection 10.1(1) or in a record obtained under subsection 10.3(2) if the Commissioner has reasonable grounds to believe that the information could be useful in the investigation of a contravention of the laws of Canada or a province that has been, is being or is about to be committed.

(7) The Commissioner may disclose information, or may authorize any person acting on behalf or under the direction of the Commissioner to disclose information, in the course of proceedings in which the Commissioner has intervened under paragraph 50(c) 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 in accordance with subsection 58(3) or 60(1) of that Act.

**21** The Commissioner or person acting on behalf or under the direction of the Commissioner is not a competent witness in respect of any matter that comes to their knowledge as a result of the



performance or exercise of any of the Commissioner's duties or powers under this Part in any proceeding other than

- (a) a prosecution for an offence under section 28;
- (b) a prosecution for an offence under section 132 of the *Criminal Code* (perjury) in respect of a statement made under this Part;
- (c) a hearing before the Court under this Part; or
- (d) an appeal from a decision of the Court.

**22 (1)** No criminal or civil proceedings lie against the Commissioner, or against any person acting on behalf or under the direction of the Commissioner, for anything done, reported or said in good faith as a result of the performance or exercise or purported performance or exercise of any duty or power of the Commissioner under this Part.

**(2)** No action lies in defamation with respect to

- (a) anything said, any information supplied or any record or thing produced in good faith in the course of an investigation or audit carried out by or on behalf of the Commissioner under this Part; and
- (b) any report made in good faith by the Commissioner under this Part and any fair and accurate account of the report made in good faith for the purpose of news reporting.

**23 (1)** If the Commissioner considers it appropriate to do so, or on the request of an interested person, the Commissioner 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 functions and duties similar to those of the Commissioner with respect to the protection of such information.

**(2)** The Commissioner may enter into agreements or arrangements with any person referred to in subsection (1) in order to

- (a) coordinate the activities of their offices and the office of the Commissioner, including to provide for mechanisms for the handling of any complaint in which they are mutually interested;
- (b) undertake and publish research or develop and publish guidelines or other instruments related to the protection of personal information;
- (c) develop model contracts or other instruments for the protection of personal information that is collected, used or disclosed interprovincially or internationally; and
- (d) develop procedures for sharing information referred to in subsection (3).

**(3)** The Commissioner may, in accordance with any procedure established under paragraph (2)(d), share information with any person referred to in subsection (1), if the information

- (a)** could be relevant to an ongoing or potential investigation of a complaint or audit under this Part or provincial legislation that has objectives that are similar to this Part; or
- (b)** could assist the Commissioner or that person in the exercise of their functions and duties with respect to the protection of personal information.

**(4)** The procedures referred to in paragraph (2)(d) shall

- (a)** restrict the use of the information to the purpose for which it was originally shared; and
- (b)** stipulate that the information be treated in a confidential manner and not be further disclosed without the express consent of the Commissioner.

**23.1 (1)** Subject to subsection (3), the Commissioner may, in accordance with any procedure established under paragraph (4)(b), disclose information referred to in subsection (2) that has come to the Commissioner's knowledge as a result of the performance or exercise of any of the Commissioner's duties or powers under this Part to any person or body who, under the legislation of a foreign state, has

- (a)** functions and duties similar to those of the Commissioner with respect to the protection of personal information; or
- (b)** responsibilities that relate to conduct that is substantially similar to conduct that would be in contravention of this Part.

**(2)** The information that the Commissioner is authorized to disclose under subsection (1) is information that the Commissioner believes

- (a)** would be relevant to an ongoing or potential 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 this Part; or
- (b)** is necessary to disclose in order to obtain from the person or body information that may be useful to an ongoing or potential investigation or audit under this Part.

**(3)** The Commissioner may only disclose information to the person or body referred to in subsection (1) if the Commissioner has entered into a written arrangement with that person or body that

- (a)** limits the information to be disclosed to that which is necessary for the purpose set out in paragraph (2)(a) or (b);
- (b)** restricts the use of the information to the purpose for which it was originally shared; and

(c) stipulates that the information be treated in a confidential manner and not be further disclosed without the express consent of the Commissioner.

**(4)** The Commissioner may enter into arrangements with one or more persons or bodies referred to in subsection (1) in order to

(a) provide for cooperation with respect to the enforcement of laws protecting personal information, including the sharing of information referred to in subsection (2) and the provision of mechanisms for the handling of any complaint in which they are mutually interested;

(b) establish procedures for sharing information referred to in subsection (2);

(c) develop recommendations, resolutions, rules, standards or other instruments with respect to the protection of personal information;

(d) undertake and publish research related to the protection of personal information;

(e) share knowledge and expertise by different means, including through staff exchanges; or

(f) identify issues of mutual interest and determine priorities pertaining to the protection of personal information.

**24** The Commissioner shall

(a) develop and conduct information programs to foster public understanding, and recognition of the purposes, of this Part;

(b) undertake and publish research that is related to the protection of personal information, including any such research that is requested by the Minister of Industry;

(c) encourage organizations to develop detailed policies and practices, including organizational codes of practice, to comply with Divisions 1 and 1.1; and

(d) promote, by any means that the Commissioner considers appropriate, the purposes of this Part.

**25 (1)** The Commissioner shall, within three months after the end of each financial year, submit to Parliament a report concerning the application of this Part, the extent to which the provinces have enacted legislation that is substantially similar to this Part and the application of any such legislation.

(2) Before preparing the report, the Commissioner shall consult with those persons in the provinces who, in the Commissioner's opinion, are in a position to assist the Commissioner in making a report respecting personal information that is collected, used or disclosed interprovincially or internationally.

**26 (1)** The Governor in Council may make regulations for carrying out the purposes and provisions of this Part, including regulations

(a) specifying, by name or by class, what is a government institution or part of a government institution for the purposes of any provision of this Part;

(a.01) [Repealed, 2015, c. 32, s. 21]

(a.1) specifying information or classes of information for the purpose of paragraph 7(1)(d), (2)(c.1) or (3)(h.1);

(b) specifying information to be kept and maintained under subsection 10.3(1); and

(c) prescribing anything that by this Part is to be prescribed.

(2) The Governor in Council may, by order,

(a) provide that this Part is binding on any agent of Her Majesty in right of Canada to which the *Privacy Act* does not apply;

(b) if satisfied that legislation of a province that is substantially similar to this Part 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 this Part in respect of the collection, use or disclosure of personal information that occurs within that province; and

(c) amend Schedule 4.

**27 (1)** Any person who has reasonable grounds to believe that a person has contravened or intends to contravene a provision of Division 1 or 1.1 may notify the Commissioner of the particulars of the matter and may request that their identity be kept confidential with respect to the notification.

(2) The Commissioner shall keep confidential the identity of a person who has notified the Commissioner under subsection (1) and to whom an assurance of confidentiality has been provided by the Commissioner.

**27.1 (1)** No employer shall dismiss, suspend, demote, discipline, harass or otherwise disadvantage an employee, or deny an employee a benefit of employment, by reason that

(a) the employee, acting in good faith and on the basis of reasonable belief, has disclosed to the Commissioner that the employer or any other person has contravened or intends to contravene a provision of Division 1 or 1.1;

(b) the employee, acting in good faith and on the basis of reasonable belief, has refused or stated an intention of refusing to do anything that is a contravention of a provision of Division 1 or 1.1;

(c) the employee, acting in good faith and on the basis of reasonable belief, has done or stated an intention of doing anything that is required to be done in order that a provision of Division 1 or 1.1 not be contravened; or

(d) the employer believes that the employee will do anything referred to in paragraph (a), (b) or (c).

(2) Nothing in this section impairs any right of an employee either at law or under an employment contract or collective agreement.

(3) In this section, *employee* includes an independent contractor and *employer* has a corresponding meaning.

**28** Every organization that knowingly contravenes subsection 8(8), section 10.1 or subsection 10.3(1) or 27.1(1) or that obstructs the Commissioner or the Commissioner's delegate in the investigation of a complaint or in conducting an audit is guilty of

(a) an offence punishable on summary conviction and liable to a fine not exceeding \$10,000; or

(b) an indictable offence and liable to a fine not exceeding \$100,000.

**\*29 (1)** The administration of this Part shall, every five years after this Part comes into force, be reviewed by the committee of the House of Commons, or of both Houses of Parliament, that may be designated or established by Parliament for that purpose.

\* [Note: Part 1 in force January 1, 2001, *see* SI/2000-29.]

(2) The committee shall undertake a review of the provisions and operation of this Part and shall, within a year after the review is undertaken or within any further period that the House of Commons may authorize, submit a report to Parliament that includes a statement of any changes to this Part or its administration that the committee recommends.

## **DIVISION 5**

### Transitional Provisions

**30 (1)** This Part does not apply to any organization in respect of personal information that it collects, uses or discloses within a province whose legislature has the power to regulate the collection, use or disclosure of the information, unless the organization does it in connection with the operation of a federal work, undertaking or business or the organization discloses the information outside the province for consideration.

(1.1) This Part does not apply to any organization in respect of personal health information that it collects, uses or discloses.

**\* (2)** Subsection (1) ceases to have effect three years after the day on which this section comes into force.

\* [Note: Section 30 in force January 1, 2001, *see* SI/2000-29.]

**\*(2.1)** Subsection (1.1) ceases to have effect one year after the day on which this section comes into force.

\* [Note: Section 30 in force January 1, 2001, *see* SI/2000-29.]

*Clause 5:* New.

*Clause 6:* Spent consequential amendments.

Aeronautics Act

*Clause 10:* Existing text of subsection 4.83(1):

**4.83 (1)** Despite section 5 of the *Personal Information Protection and Electronic Documents Act*, to the extent that that section relates to obligations set out in Schedule 1 to that Act relating to the disclosure of information, and despite subsection 7(3) of that Act, an operator of an aircraft departing from Canada that is due to land in a foreign state or fly over the United States and land outside Canada or of a Canadian aircraft departing from any place outside Canada that is due to land in a foreign state or fly over the United States may, in accordance with the regulations, provide to a competent authority in that foreign state any information that is in the operator's control relating to persons on board or expected to be on board the aircraft and that is required by the laws of the foreign state.

Canadian Radio-television and Telecommunications Commission Act

*Clause 13:* New.

Competition Act

*Clause 14:* New.

Canada Business Corporations Act

*Clause 15:* Existing text of subsection 21.1(5):

**(5)** Within one year after the sixth anniversary of the day on which an individual ceases to be an individual with significant control over the corporation, the corporation shall — subject to any other Act of Parliament and to any Act of the legislature of a province that provides for a longer retention period — dispose of any of that individual's *personal information*, as defined in subsection 2(1) of the *Personal Information Protection and Electronic Documents Act*, that is recorded in the register.

[Telecommunications Act](#)

[Clause 16: \(1\) Existing text of subsection 39\(2\):](#)

[\(2\) Subject to subsections \(4\), \(5\), \(5.1\) and \(6\), where a person designates information as confidential and the designation is not withdrawn by that person, no person described in subsection \(3\) shall knowingly disclose the information, or knowingly allow it to be disclosed, to any other](#)

person in any manner that is calculated or likely to make it available for the use of any person who may benefit from the information or use the information to the detriment of any person to whose business or affairs the information relates.

(2) New.

Public Servants Disclosure Protection Act

Clause ~~16~~17: Relevant portion of section 15:

**15** Sections 12 to 14 apply despite

(a) section 5 of the *Personal Information Protection and Electronic Documents Act*, to the extent that that section relates to obligations set out in Schedule 1 to that Act relating to the disclosure of information; and

Clause ~~17~~18: Existing text of subsection 16(1.1):

**(1.1)** Subsection (1) does not apply in respect of information the disclosure of which is subject to any restriction created by or under any Act of Parliament, including the *Personal Information Protection and Electronic Documents Act*.

Clause ~~18~~19: Existing text of section 50:

**50** Despite section 5 of the *Personal Information Protection and Electronic Documents Act*, to the extent that that section relates to obligations set out in Schedule 1 to that Act relating to the disclosure of information, and despite any other Act of Parliament that restricts the disclosure of information, a report by a chief executive in response to recommendations made by the Commissioner to the chief executive under this Act may include personal information within the meaning of subsection 2(1) of that Act, or section 3 of the *Privacy Act*, depending on which of those Acts applies to the portion of the public sector for which the chief executive is responsible.

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

Clause ~~19~~20: Existing text of section 2:

**2** In the event of a conflict between a provision of this Act and a provision of Part 1 of the *Personal Information Protection and Electronic Documents Act*, the provision of this Act operates despite the provision of that Part, to the extent of the conflict.

Clause ~~20~~21: Relevant portion of subsection 20(3):

**(3)** The following factors must be taken into account when determining the amount of a penalty:

...

(c) the person's history with respect to any previous violation under this Act, any previous conduct that is reviewable under section 74.011 of the *Competition Act* and any previous contravention of section 5 of the *Personal Information Protection and Electronic Documents Act* that relates to a collection or use described in subsection 7.1(2) or (3) of that Act;

Clause ~~21~~22: ~~Text~~Existing text of subsection 47(1):

**47 (1)** A person who alleges that they are affected by an act or omission that constitutes a contravention of any of sections 6 to 9 of this Act or of section 5 of the *Personal Information Protection and Electronic Documents Act* that relates to a collection or use described in subsection 7.1(2) or (3) of that Act — or that constitutes conduct that is reviewable under section 74.011 of the *Competition Act* — may apply to a court of competent jurisdiction for an order under section 51 against one or more persons who they allege have committed the act or omission or who they allege are liable for the contravention or reviewable conduct by reason of section 52 or 53.

(2) ~~Text~~Existing text of subsection 47(4):

(4) The applicant must, without delay, serve a copy of the application on every person against whom an order is sought, on the Commission if the application identifies a contravention of this Act, on the Commissioner of Competition if the application identifies conduct that is reviewable under section 74.011 of the *Competition Act* and on the Privacy Commissioner if the application identifies a contravention of the *Personal Information Protection and Electronic Documents Act*.

Clause ~~22~~23: Relevant portion of section 50:

**50** The following may intervene in any proceedings in connection with an application under subsection 47(1) for an order under paragraph 51(1)(b) and in any related proceedings:

...

(c) the Privacy Commissioner, if the application identifies a contravention of the *Personal Information Protection and Electronic Documents Act*.

Clause ~~23~~24: Relevant portion of subsection 51(1):

**51 (1)** If, after hearing the application, the court is satisfied that one or more persons have contravened any of the provisions referred to in the application or engaged in conduct referred to in it that is reviewable under section 74.011 of the *Competition Act*, the court may order the person or persons, as the case may be, to pay the applicant

...

(b) a maximum of

...



(vi) in the case of a contravention of section 5 of the *Personal Information Protection and Electronic Documents Act* that relates to a collection or use described in subsection 7.1(2) or (3) of that Act, \$1,000,000 for each day on which a contravention occurred, and

(2) Text of subsection 51(2):

(2) The purpose of an order under paragraph (1)(b) is to promote compliance with this Act, the *Personal Information Protection and Electronic Documents Act* or the *Competition Act*, as the case may be, and not to punish.

(2) Relevant portion of subsection 51(3):

(3) The court must consider the following factors when it determines the amount payable under paragraph (1)(b) for each contravention or each occurrence of the reviewable conduct:

...

(c) the person's history, or each person's history, as the case may be, with respect to any previous contravention of this Act and of section 5 of the *Personal Information Protection and Electronic Documents Act* that relates to a collection or use described in subsection 7.1(2) or (3) of that Act and with respect to any previous conduct that is reviewable under section 74.011 of the *Competition Act*;

Clause ~~2425~~: Existing text of sections 52 to 54:

**52** An officer, director, agent or mandatary of a corporation that commits a contravention of any of sections 6 to 9 of this Act or of section 5 of the *Personal Information Protection and Electronic Documents Act* that relates to a collection or use described in subsection 7.1(2) or (3) of that Act, or that engages in conduct that is reviewable under section 74.011 of the *Competition Act*, is liable for the contravention or reviewable conduct, as the case may be, if they directed, authorized, assented to, acquiesced in or participated in the commission of that contravention, or engaged in that conduct, whether or not the corporation is proceeded against.

**53** A person is liable for a contravention of any of sections 6 to 9 of this Act or of section 5 of the *Personal Information Protection and Electronic Documents Act* that relates to a collection or use described in subsection 7.1(2) or (3) of that Act, or for conduct that is reviewable under section 74.011 of the *Competition Act*, that is committed or engaged in, as the case may be, by their employee acting within the scope of their employment or their agent or mandatary acting within the scope of their authority, whether or not the employee, agent or mandatary is identified or proceeded against.

**54 (1)** A person must not be found to have committed a contravention of any of sections 6 to 9 of this Act or of section 5 of the *Personal Information Protection and Electronic Documents Act* that relates to a collection or use described in subsection 7.1(2) or (3) of that Act, or to have engaged in conduct that is reviewable under section 74.011 of the *Competition Act*, if they establish that they exercised due diligence to prevent the contravention or conduct, as the case may be.

(2) Every rule and principle of the common law that makes any circumstance a justification or excuse in relation to a charge for an offence applies in respect of a contravention of any of sections 6 to 9 of this Act or of section 5 of the *Personal Information Protection and Electronic Documents Act* that relates to a collection or use described in subsection 7.1(2) or (3) of that Act, or in respect of conduct that is reviewable under section 74.011 of the *Competition Act*, to the extent that it is not inconsistent with this Act or the *Personal Information Protection and Electronic Documents Act* or the *Competition Act*, as the case may be.

Clause ~~25~~26: (1) and (2) Relevant portion of section 56:

**56** Despite subsection 7(3) of the *Personal Information Protection and Electronic Documents Act*, any organization to which Part 1 of that Act applies may on its own initiative disclose to the Commission, the Commissioner of Competition or the Privacy Commissioner any information in its possession that it believes relates to

(a) a contravention of

...

(iii) section 5 of the *Personal Information Protection and Electronic Documents Act*, which contravention relates to a collection or use described in subsection 7.1(2) or (3) of that Act, or

Clause ~~26~~27: Existing text of section 57:

**57** The Commission, the Commissioner of Competition and the Privacy Commissioner must consult with each other to the extent that they consider appropriate to ensure the effective regulation, under this Act, the *Competition Act*, the *Personal Information Protection and Electronic Documents Act* and the *Telecommunications Act*, of commercial conduct that discourages the use of electronic means to carry out commercial activities, and to coordinate their activities under those Acts as they relate to the regulation of that type of conduct.

Clause ~~27~~28: (1) Relevant portion of subsection 58(1):

**58 (1)** The Commission may disclose information obtained by it in the performance or exercise of its duties or powers related to any of sections 6 to 9 of this Act and, in respect of conduct carried out by electronic means, to section 41 of the *Telecommunications Act*,

(a) to the Privacy Commissioner, if the Commission believes that the information relates to the performance or exercise of the Privacy Commissioner's duties or powers under Part 1 of the *Personal Information Protection and Electronic Documents Act* in respect of a collection or use described in subsection 7.1(2) or (3) of that Act; and

(2) Relevant portion of subsection 58(2):

(2) Despite section 29 of the *Competition Act*, the Commissioner of Competition may disclose information obtained by him or her in the performance or exercise of his or her duties or powers related to section 52.01 or 74.011 of that Act or, in respect of conduct carried out by electronic means, to section 52, 52.1, 53, 55, 55.1, 74.01, 74.02, 74.04, 74.05 or 74.06 of that Act,

(a) to the Privacy Commissioner, if the Commissioner of Competition believes that the information relates to the performance or exercise of the Privacy Commissioner's duties or powers under Part 1 of the *Personal Information Protection and Electronic Documents Act* in respect of a collection or use described in subsection 7.1(2) or (3) of that Act; and

(3) Relevant portion of subsection 58(3):

(3) The Privacy Commissioner may disclose information obtained by him or her in the performance or exercise of his or her duties or powers under Part 1 of the *Personal Information Protection and Electronic Documents Act* if the information relates to a collection or use described in subsection 7.1(2) or (3) of that Act or to an act alleged in a complaint in respect of which the Privacy Commissioner decides, under subsection 12(2) or 12.2(2) of that Act, to not conduct an investigation or to discontinue an investigation,

Clause ~~2829~~2829: Existing text of subsection 59(3):

(3) The Privacy Commissioner may use the information that is disclosed to him or her under paragraph 58(1)(a) or (2)(a) only for the purpose of performing or exercising his or her duties or powers under

Part 1 of the *Personal Information Protection and Electronic Documents Act* in respect of a collection or use described in subsection 7.1(2) or (3) of that Act.

Clause ~~2930~~2930: (1) and (2) Relevant portion of subsection 60(1):

**60 (1)** Information may be disclosed under an agreement or arrangement in writing between the Government of Canada, the Commission, the Commissioner of Competition or the Privacy Commissioner and the government of a foreign state, an international organization of states or an international organization established by the governments of states, or any institution of any such government or organization, if the person responsible for disclosing the information believes that

(a) the information may be relevant 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

...

(ii) conduct that contravenes section 5 of the *Personal Information Protection and Electronic Documents Act* and that relates to a collection or use described in subsection 7.1(2) or (3) of that Act,

(b) the disclosure is necessary in order to obtain from that foreign state, organization or institution information that may be relevant for any of the following purposes and no more information will be disclosed than is required for that purpose:

...

(iii) the performance or exercise by the Privacy Commissioner of his or her duties or powers under Part 1 of the *Personal Information Protection and Electronic Documents Act* in respect of a collection or use described in subsection 7.1(2) or (3) of that Act, or

Clause ~~30~~31: Existing text of section 61:

**61** The Commission, the Commissioner of Competition and the Privacy Commissioner must provide the Minister of Industry with any reports that he or she requests for the purpose of coordinating the implementation of sections 6 to 9 of this Act, sections 52.01 and 74.011 of the *Competition Act* and section 7.1 of the *Personal Information Protection and Electronic Documents Act*.

Transportation Modernization Act

Clause ~~31~~32: Existing text of subsection 17.91(4):

(4) A company that collects, uses or communicates information under this section, section 17.31 or 17.94, subsection 28(1.1) or 36(2) or regulations made under section 17.95 may do so

(a) despite section 5 of the *Personal Information Protection and Electronic Documents Act*, to the extent that that section relates to obligations set out in Schedule 1 to that Act relating to the collection, use, disclosure and retention of information, and despite section 7 of that Act; and

(b) despite any provision of provincial legislation that is substantially similar to Part 1 of the Act referred to in paragraph (a) and that limits the collection, use, communication or preservation of information.

Document comparison by Workshare 10.0 on Thursday, June 23, 2022 2:10:51 PM

Input:	
Document 1 ID	file://H:\Files\CLIENTS for NetDocs\CDR\Bill C-27\1. Bill C-11 First Reading Nov 17 2020 (EN).docx
Description	1. Bill C-11 First Reading Nov 17 2020 (EN)
Document 2 ID	file://H:\Files\CLIENTS for NetDocs\CDR\Bill C-27\1. Bill C-27 First Reading June 16 2022 (EN).docx
Description	1. Bill C-27 First Reading June 16 2022 (EN)
Rendering set	Standard

Legend:	
<u>Insertion</u>	
<del>Deletion</del>	
<del>Moved from</del>	
<u>Moved to</u>	
Style change	
Format change	
<del>Moved deletion</del>	
Inserted cell	
Deleted cell	
Moved cell	
Split/Merged cell	
Padding cell	

Statistics:	
	Count
Insertions	877
Deletions	412
Moved from	22
Moved to	22
Style change	0
Format changed	0
Total changes	1333