Cassels

PIPEDA Reimagined – Federal Privacy Law Modernization, Take Two

Bernice Karn, Courtney Wong, Marco Ciarlariello, Shae Rothery

June 28, 2022

Digital Charter Implementation Act, 2022
1

Bill C-11

- Create the *Consumer Privacy Protection Act* (CPPA), replacing Part 1 of the *Personal Information Protection and Electronic Documents Act* (PIPEDA),[2] Canada's current private sector privacy law.
- Create the *Personal Information and Data Protection Tribunal Act* (PIDPTA), which would establish a tribunal that would hear the Office of the Privacy Commissioner of Canada's (OPC's) recommendations on administrative monetary penalties and appeals from certain inquiry findings and compliance orders of the OPC.
- Enact the *Artificial Intelligence and Data Act* (AIDA) to regulate "international and interprovincial trade and commerce in AI systems" and prohibit certain conduct that could result in serious harm to individuals and their interests.[3]

here

here

The Consumer Privacy Protection Act (CPPA) - The Highlights

Shift in Focus

recognizing

taking into account

Anonymized vs. De-identified Information

4

5

Legitimate Interests

Consent

Collection, Retention, and Disposal of Personal Information

6

purposes

manner of collection

7

8

9

collected

under the organization's control

ensure

Minors

Cross-border Transfers

adequacy ruling with the EU

Charities and Political Parties

Substantial Penalties

Newly added sections in Bill C-27 where administrative monetary penalties may be imposed[10]

Subsection 9(1)	Implementation and maintenance of a privacy management program that includes policies, practices, and procedures.

Subsection 11(1)	Requirement to guarantee that service providers give a level of protection which is equivalent to the level of protection that the transferring organization is required to provide.
Subsection 12(3)	Requirement to determine the reason for which the personal information is being collected, used, or disclosed and to record those purposes before using or disclosing that information.
Subsection 12(4)	For any new purpose, the organization must record that new purposes before using or disclosing information for that new purpose.
Subsections 15(1) and (7)	Requirement that an organization obtains a person's valid consent for the collection, use or disclosure of the person's personal information, unless it falls within an exception.
Subsection 17(2)	Requirement that when receiving a request to withdraw consent, the organization must inform the person of the consequences associated with the withdrawal of their consent, and cease the collection, use or disclosure of the person's personal information.
Subsections 55(1) and (4)	Requirement to dispose of the information upon request by individual and a need to inform service providers to whom the organization has transferred the information.
Section 61	Requirement that if service providers face data breaches, they must notify the organization that controls the personal information.
Subsection 62(1)	Requirement that the information explaining the organization's policies and practices be made readily available, and in plain language.

11

Expansion of the OPC's Powers

12

13

14

The Personal Information and Data Protection Tribunal Act (PIDPTA)

here

Inquiries Act

15

16

17

The Artificial Intelligence and Data Act (AIDA)

Artificial Intelligence and Data Act

18

autonomous or semi-autonomous

Requirements for Persons Responsible for AI Systems

- **Anonymized Data:** persons who carry out regulated activities and make anonymized data available for use in AI systems must establish measures with respect to the manner in which those data are anonymized and the use or management of anonymized data.[19]
- **Assessments of High Impact Systems**: persons responsible for AI systems must assess whether they are high-impact systems.[20]
- **Risk Mitigation:** persons responsible for high impact systems must establish measures to identify, assess, and mitigate risks of harm or biased output that could result from use of the system.[21] These risk mitigation measures and their effectiveness must also be monitored.[22]
- **Keeping General Records:** persons who carry out any regulated activities must keep records for measures related to anonymized data and risk mitigation, and reasons that support their assessment of the AI system for which they are responsible as a high-impact system.[23]
- **Plain-Language Public Disclosure:** persons who make available or manage the operation of a high-impact AI system must publish, on a publicly available website, plain-language descriptions that include descriptions of (a) how the system is intended to be or is used, (b) the types of content that the system is intended to generate or does generate and the decisions, recommendations, or predictions that it is intended to or does make, (c) mitigation measures taken to reduce the risk of harm or biased output, as required by section 8 of the AIDA, and (d) other information prescribed by regulation.[24] Additionally, persons that are responsible for high-impact systems must notify the Minister if use of the system results in or is likely to result in material harm, which is characterized as physical or psychological harm to an individual, damage to an individual's property, or economic loss to an individual.[25]

Powers of the Minister

26

27

28

29

Administrative Monetary Penalties

30

31

- **On conviction on indictment:**
  - Fine of not more than the greater of C$10 million 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, OR a fine at the discretion of the court, in the case of an individual
- **On conviction on summary conviction:**
  - Fine of not more than the greater of C$5 million 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, OR a fine of not more than $50,000, in the case of an individual

32

33

Criminal Offences

- **Possession or use of personal information:** It is an offence if a person, if for the purpose of designing, developing, using, or making available for use an AI system, the person possesses or uses personal information, knowing or believing that the information is obtained or derived, directly or indirectly, as a result of (a) an offence under an Act of Parliament or provincial legislature, or (b) an act or omission anywhere that, if it had occurred in Canada, would have constituted such an offence.[34]
- **Making an AI system available for use:** It is an offence if the person knows or is reckless as to

whether use of an AI system is likely to cause serious physical or psychological harm to an individual or substantial damage to an individual's property, makes the AI system available for use and the system causes such harm, OR with intent to defraud public and cause substantial economic loss to an individual, makes an AI system available and causes that loss.[35]

[36]

- **On conviction on indictment:**
  - Fine of not more than the greater of C$25 million 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, OR a fine at the discretion of the court or term of imprisonment of up to 5 years less a day or both, in the case of an individual.
- **On conviction on summary conviction:**
  - Fine of not more than the greater of C$20 million 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, OR a fine of not more than $100,000 or a term of imprisonment of up to two years less a day, or both, in the case of an individual.

Going Forward

[1] Bill C-27, *An Act to enact the Consumer Privacy Protection Act, the Personal Information and Data Protection Tribunal Act and the Artificial Intelligence and Data Act and to make consequential and related amendments to other Acts*, 1st Sess, 44th Parl, 2022 (first reading 16 June 2022) ["Bill C-27"].

[2] *Personal Information Protection and Electronics Documents Act*, SC 2000, c 5 ["PIPEDA"].

[3] Bill C-27, *supra* note 1 at Part 3, cl 4.

[4] *Ibid* at Part 1, cl 2.

[5] *Ibid*.

[6] PIPEDA, *supra* note 2 at Part 1, cl 5(3).

[7] Bill C-27, *supra* note 1 at Part 1, cl 12(1).

[8] *Ibid* at Part 1, cl 53(2).

[9] *Ibid* at Part 1, cl 62(2)(e).

[10] *Ibid* at Part 1, cl 94(1).

[11] *Ibid* at Part 1, cl 107.

[12] *Ibid* at Part 1, cl 89, 90 and 94.

[13] *Ibid* at Part 1, cl 116.

[14] *Ibid* at Part 1, cl 109.

[15] *Ibid* at Part 2, cl 16(1).

[16] *Ibid* at Part 2, cl 16(2).

[17] *Ibid* at Part 2, cl 16(3).

[18] *Ibid* at Part 3, cl 2.

[19] *Ibid* at Part 3, cl 6.

[20] *Ibid* at Part 3, cl 7.

[21] *Ibid* at Part 3, cl 8.

[22] *Ibid* at Part 3, cl 9.

[23] *Ibid* at Part 3, cl 10.

[24] *Ibid* at Part 3, cl 11(1) and (2).

[25] *Ibid* at Part 3, cl 12.

[26] *Ibid* at Part 3, cl 13 & 14.

[27] *Ibid* at Part 3, cl 15 & 16.

[28] *Ibid* at Part 3, cl 17.

[29] *Ibid* at Part 3, cl 28.

[30] *Ibid* at Part 3, cl 29(2).

[31] *Ibid* at Part 3, cl 30.

[32] *Ibid* at Part 3, cl 30(4).

[33] *Ibid* at Part 3, cl 30(5).

[34] *Ibid* at Part 3, cl 38.

[35] *Ibid* at Part 3, cl 39.

[36] *Ibid* at Part 3, cl 40.
