mccarthy tétrault

CPPA: Canada's proposed new privacy law: summary and criticisms

Barry B. Sookman
McCarthy Tétrault LLP
bsookman@mccarthy.ca
416-601-7949

April 22, 2021

21393197

What is the *Digital Charter Implementation Act, 2020* (Bill C-11)

To enact the *Consumer Privacy Protection Act* (CPPA)

"to protect 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* "

Part of federal ISED new Digital Charter strategy to address new challenges, e.g. AI, IOT, clarify uncertainties, and to maintain Canada's EU GDPR adequacy status, react to provincial proposals.

Status of Bill: 2nd Reading April 19, 2021.

To enact the *Personal Information and Data Protection Tribunal Act*

"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."

CPPA

Only part of Canada's privacy fractured landscape

Must fit into fractured international privacy landscape

Fact Sheet: Digital Charter Implementation Act, 2020

Through the proposed Digital Charter Implementation Act, 2020 (DCIA), the Government of Canada intends to establish a new privacy law for the private sector, the Consumer Privacy Protection Act (CPPA). If passed, the DCIA would significantly increase protections to Canadians' personal information by giving Canadians more control and greater transparency when companies handle their personal information. The DCIA would also provide significant new consequences for non-compliance with the law, including steep fines for violations.

Fact Sheet: Digital Charter Implementation Act, 2020

Strengthened enforcement and oversight

—**Comprehensive and accessible enforcement model:** Under the CPPA, the Privacy Commissioner would have broad order-making powers, including the ability to force an organization to comply with its requirements under the CPPA and the ability to order a company to stop collecting data or using personal information. In addition, the Privacy Commissioner would also be able to recommend that the Personal Information and Data Protection Tribunal impose a fine. The legislation would provide for administrative monetary penalties of up to 3% of global revenue or $10 million for non-compliant organizations. It also contains an expanded range of offences for certain serious contraventions of the law, subject to a maximum fine of 5% of global revenue or $25 million.

—**What about social media?** Social media platforms are already subject to the same laws as other organizations operating in the Canadian marketplace. The CPPA would ensure that Canadians have the ability to demand that their information on these platforms be permanently deleted. When consent is withdrawn or information is no longer necessary, Canadians can demand that their information be destroyed. To reinforce this, the Privacy Commissioner will have the ability to order a social media company to comply, including order it to stop collecting data or using personal information.

What does the Digital Charter Implementation Act, 2020 mean for me?

Meaningful consent: Modernized consent rules would ensure that individuals have the plain-language information they need to make meaningful choices about the use of their personal information.

Data mobility: To further improve their control, individuals would have the right to direct the transfer of their personal information from one organization to another. For example, individuals could direct their bank to share their personal information with another financial institution.

Disposal of personal information and withdrawal of consent: The accessibility of information online makes it hard for individuals to control their online identity. The legislation would allow individuals to request that organizations dispose of personal information and, in most cases, permit individuals to withdraw consent for the use of their information.

What does the Digital Charter Implementation Act, 2020 mean for me?

Algorithmic transparency: The CPPA contains new transparency requirements that apply to automated decision-making systems like algorithms and artificial intelligence. Businesses would have to be transparent about how they use such systems to make significant predictions, recommendations or decisions about individuals. Individuals would also have the right to request that businesses explain how a prediction, recommendation or decision was made by an automated decision-making system and explain how the information was obtained.

De-identified information: The practice of removing direct identifiers (such as a name) from personal information is becoming increasingly common, but the rules that govern how this information is then used are not clear. The legislation will clarify that this information must be protected and that it can be used without an individual's consent only under certain circumstances.

Criticisms of CPPA

- PIPEDA is principle based and flexible, CPPA is more prescriptive and rule based e.g. consents
- CPPA creates ambiguous new standards that are difficult to apply e.g. appropriate purposes limitation, standards and exceptions for consent, explainability of decisions and predictions using automated decisions, what is a commercial activity
- CPPA is more onerous than international standards including even aspects GDPR e.g. consent and exceptions to consent such as for R&D, de-identified information, automated decisions, the disposal/erasure of data, service provider obligations
- CPPA creates obligations that eschew/challenge technological means of compliance e.g. disposal of information, explainability of decisions using automated decision systems
- CPPA has some harsher penalties than even the GDPR, weak procedural protections, new private rights of action and with new class action risks
- Harsh penalties could impede risk taking and innovation, especially when combined with onerous/ambiguous standards
- CPPA is not interoperable with GDPR, provincial or other international standards
- Overall balance in CPPA requires recalibration to promote privacy and not impede innovation or prejudice Canadian based businesses

mccarthy tétrault

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~~course 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~~ commercial activities

Purpose of CPPA

~~3~~5 The purpose of this ~~Part~~ Act is to establish~~,~~ — in an era in which ~~technology increasingly facilitates the~~ 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 ~~collection, use and disclosure~~ 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 of CCPA

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)(b)

Application of CCPA

(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;

Application of CCPA

(4) This Act does not apply to…

(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(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.

~~**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.~~

What CPPA Applies to

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~~ 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.

personal information means information about an identifiable individual. (*renseignement personnel*)

Appropriate Purposes Limitation

CPPA s. 12 (1) An organization may collect, use or disclose personal information only for purposes that a reasonable person would consider appropriate in the circumstances.

(2) The following factors must be taken into account in determining whether the 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 any measures, technical or otherwise, implemented by the organization to mitigate the impacts of the loss of privacy on the individual.

(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.

(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.

Consent

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.

(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.

(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 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.

(4) Consent must be expressly obtained, unless the organization establishes that 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.

False Statements when obtaining consent

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.

Exceptions from consent

Business Operations

— 18 Business activities

— 19 Transfer to service provider

— 20 De-identification of personal information

— 21 Research 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

No exception for legitimate interests as under GDPR

— Art. 6(1)(f) “processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child”.

— UK ICO “Legitimate interests is the most flexible lawful basis for processing, but you cannot assume it will always be the most appropriate. It is likely to be most appropriate where you use people’s data in ways they would reasonably expect and which have a minimal privacy impact, or where there is a compelling justification for the processing.”

— Recital 47 “Such legitimate interest could exist for example where there is a relevant and appropriate relationship between the data subject and the controller in situations such as where the data subject is a client or in the service of the controller…. The processing of personal data strictly necessary for the purposes of preventing fraud also constitutes a legitimate interest of the data controller concerned. The processing of personal data for direct marketing purposes may be regarded as carried out for a legitimate interest.”

— Recital 48 “Controllers that are part of a group of undertakings or institutions affiliated to a central body may have a legitimate interest in transmitting personal data within the group of undertakings for internal administrative purposes, including the processing of clients' or employees' personal data.”

— Recital 49 “for the purposes of ensuring network and information security” including “preventing unauthorised access to electronic communications networks and malicious code distribution and stopping ‘denial of service’ attacks and damage to computer and electronic communication systems”.

— Will the CPPA permit: monitoring and analyzing performance of a product; improving or developing a product; personalizing experiences within a product where these experiences are part of the product or service; making recommendations within a product or service; disclosing personal information to affiliates, dealers, franchisees or channel partners. See Submission of TECHNATION to ISED.

Exceptions from consent – business operations

Business Operations

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 a business activity described in subsection (2) and

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

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

(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

any other prescribed activity.

Exceptions for consent – de-identification

- **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 an individual or could not be used in reasonably foreseeable circumstances, alone or in combination with other information, to identify an individual.

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

- **75** An organization must not use de-identified information alone or in combination with other information to identify an individual, except in order to conduct testing of the effectiveness of security safeguards that the organization has put in place to protect the information.

- Unlike under PIPEDA and the GDPR, anonymized information is subject to the CPPA. Instead, CPPA has 3 narrow exceptions where PI has been de-identified:

  - **S.21** internal research and development

  - **S.22(1)** prospective business transactions

  - **S.39(1)** disclosures for a socially beneficial purpose.

- **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.

Exceptions for consent – business transactions

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 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.

Exceptions for consent – business transactions

Completed business transaction

(2) 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 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

(3) 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.

Exceptions for consent – R&D

- **Research and development**

- **21** An organization may use an individual's personal information without their knowledge or consent for the organization's internal research and development purposes, if the information is de-identified before it is used.

- GDPR See, IAPP, How GDPR changes the rules for research. "Research occupies a privileged position within the Regulation. Organizations that process personal data for research purposes may avoid restrictions on secondary processing and on processing sensitive categories of data (Article 6(4); Recital 50). As long as they implement appropriate safeguards, these organizations also may override a data subject's right to object to processing and to seek the erasure of personal data (Article 89)." GDPR Recital 26 "This Regulation does not therefore concern the processing of such anonymous information, including for statistical or research purposes."

- Recital 50 "Further processing for… scientific or historical research purposes or statistical purposes should be considered to be compatible lawful processing operations."

- GDPR 1(b) Personal data "collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes"

- GDPR Art 89(1) Processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, shall be subject to appropriate safeguards, in accordance with this Regulation, for the rights and freedoms of the data subject. Those safeguards shall ensure that technical and organisational measures are in place in particular in order to ensure respect for the principle of data minimisation. Those measures may include pseudonymisation provided that those purposes can be fulfilled in that manner".

Service Providers

"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.

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

s.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 protection of the personal information as that which the organization is required to provide under this Act.

(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.

s. 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.

s. 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.

Service Providers

—PIPEDA required a comparable level of protection

—CPPA imposes different standards on service providers with multiple customers:

  —s.11(1), “substantially the same protection of the personal information as that which the organization is required to provide under this Act”;

  —the generally applicable security safeguards standards under s 57.

—Under Article 28 of the GDPR where “processing is to be carried out on behalf of a controller, the controller shall use only processors providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that processing will meet the requirements of this Regulation and ensure the protection of the rights of the data subject.”

Exceptions from consent – collecting in the course of employment

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.

Exception for publicly available

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.

Withdrawing consent

CPPA s. 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.

(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.

PIPEDA: principle 4.3.8 "An individual may withdraw consent at any time, subject to legal or contractual restrictions and reasonable notice. The organization shall inform the individual of the implications of such withdrawal."

Disposal of information (erasure)

disposal means the permanent and irreversible deletion of personal information.

55 (1) If an organization receives a written request from an individual to dispose of personal information that it has collected from the individual, the organization must, as soon as feasible, dispose of the information, unless

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

(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.

(2) An organization that 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).

(3) If an organization disposes of personal information, 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 the service provider that the information has been disposed of.

Disposal of information (erasure)

PIPEDA Principle 4.5.3 “Personal information that is no longer required to fulfil the identified purposes should be destroyed, erased, or made anonymous. Organizations shall develop guidelines and implement procedures to govern the destruction of personal information.”

GDPR right of erasure is more limited and has more exceptions, for example:

—(a) the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed;

—(b) the data subject withdraws consent on which the processing is based according to point (a) of Article 6(1), or point (a) of Article 9(2), and where there is no other legal ground for the processing;

—(c) the data subject objects to the processing pursuant to Article 21(1) and there are no overriding legitimate grounds for the processing, or the data subject objects to the processing pursuant to Article 21(2)

GDPR has other exceptions: e.g. for exercising the right of freedom of expression and information, for compliance with a legal obligation; for … scientific or historical research purposes or statistical purposes in accordance with Article 89(1) in so far as the right referred to in paragraph 1 is likely to render impossible or seriously impair the achievement of the objectives of that processing; or for the establishment, exercise or defence of legal claims.

Retention of information

53 An organization must not retain personal information for a period longer than necessary to

(a) fulfil 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.

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.

Privacy Management Program

CPPA s. 9 (1) Every organization must implement a privacy management program that includes the organization's policies, practices and procedures put in place to fulfil 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.

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

Accountability

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

(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.

4.1.1 Accountability for the organization's compliance with the principles rests with the designated individual(s), even though other individuals within the organization may be responsible for the day-to-day collection and processing of personal information. In addition, other individuals within the organization may be delegated to act on behalf of the designated individual(s).

4.1.2 The identity of the individual(s) designated by the organization to oversee the organization's compliance with the principles shall be made known upon request.

4.1.4 Organizations shall implement policies and practices to give effect to the principles, including implementing procedures to protect personal information; establishing procedures to receive and respond to complaints and inquiries; training staff and communicating to staff information about the organization's policies and practices; and developing information to explain the organization's policies and procedures.

Limiting Collection

4 Principle 4 — Limiting Collection

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

Limiting Use, Disclosure, and Retention

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.

(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 (2) and sections 23, 24, 26, 30, 41 and 51; or

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 (2), sections 23 to 28, 31 to 37 and 39, subsection 40(3) and sections 42 and 43 to 51.

Automated decision making

automated decision system means any technology that assists or replaces the judgement of human decision-makers using techniques such as rules-based systems, regression analysis, predictive analytics, machine learning, deep learning and neural nets.

CPPA 62 (1) Transparency/openness obligation for Automated decision system: an organization must make the following information available

(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 significant impacts on them;

63 (1) Data access/explainability obligation for Automated decision system : On request by an individual:

(3) If the organization has used an automated decision system to make a prediction, recommendation or decision about the individual, the organization must, on request by the individual, provide them with an explanation of the prediction, recommendation or decision and of how the personal information that was used to make the prediction, recommendation or decision was obtained.

Automated decision making

GDPR: Subject to exceptions, under Art. 22 "The data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her.

Transparency and explainability under the GDPR:

Articles 14(1)(2)(g) and 15(1)(h): "The data subject shall have the right to obtain form the controller confirmation [of] … the following information: (h) the existence of automated decision-making, including profiling, referred to in Article 22(1)… and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject."

Data mobility

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.

Accuracy

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 the purposes for which the information is collected, used or disclosed.

(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 fulfil the purposes for which the information is collected, used or disclosed.

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.

(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.

(3) The security safeguards must protect personal information against, among other things, loss, theft and unauthorized access, disclosure, copying, use and modification. (Note re-written)

Safeguards (PIPEDA)

4.7 Principle 7 — Safeguards Personal information shall be protected by security safeguards appropriate to the sensitivity of the information.

4.7.1 The security safeguards shall protect personal information against loss or theft, as well as unauthorized access, disclosure, copying, use, or modification. Organizations shall protect personal information regardless of the format in which it is held.

4.7.2 The nature of the safeguards will vary depending on the sensitivity of the information that has been collected, the amount, distribution, and format of the information, and the method of storage. More sensitive information should be safeguarded by a higher level of protection. The concept of sensitivity is discussed in Clause 4.3.4.

Transparency/Openness

CPPA 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 its obligations under this Act.

(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 personal information, including how the organization applies the exceptions to the requirement to obtain consent under this Act;

(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 significant impacts 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) how an individual may make a request for disposal under section 55 or access under section 63; and

(f) the business contact information of the individual to whom complaints or requests for information may be made.(re-written)

Codes of Practice

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 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.

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.

Certification programs

77 (1) An entity may, in the manner provided by 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.

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.

Enforcement and Remedies

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;

(b) on behalf of a deceased individual by a person authorized by or under law to administer the estate or succession of that individual, but only for the purpose of that administration; and

(c) on behalf of any other individual by any person authorized in writing to do so by the individual.

OPC Investigation of complaints

90 (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.

(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.

(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.

91 The Commissioner may determine the procedure to be followed in the conduct of an inquiry and must make that procedure publicly available.

Powers of the Commissioner

92 (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); and

(d) the Commissioner's reasons for the findings, order or decision.

(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 its obligations under this Act.

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

(4) An inquiry conducted under section 88 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.

Powers of Commissioner

98 (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.

(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.

Recommendations of Penalties

93 (1) If, in completing an inquiry under section 88 or 89, 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) section 13; (limiting collection of personal information)

(b) subsection 14(1); (using information for a new purpose w/o consent)

(c) subsection 15(5); (requiring consents to obtain a product)

(d) section 16; (obtaining information by fraud or misleading information)

(e) section 53; (disposal/retention of information for longer than needed)

(f) subsections 55(1) and (3); (disposal/erasure obligations)

(g) subsection 57(1); (breach of security safeguards)

(h) subsections 58(1) and (3). (breach notifications to OPC and individuals)

Recommendations of Penalties

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

(a) the nature and scope of the contravention;

(b) whether the organization has voluntarily paid compensation to a person affected by the contravention;

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

(d) any other relevant factor.

(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).

(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) that sets out the decision to recommend.

Focus of the Commissioner

108 In addition to taking into account the purpose of this Act in the exercise of the Commissioner's powers and the performance of the Commissioner's duties and functions under this Act, the Commissioner must take into account the size and revenue of organizations, the volume and sensitivity of the personal information under their control and matters of general public interest.

Powers of the Tribunal

94 (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) 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…

(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) 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.

(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.

102 (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.

s.102(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.

Powers of the Tribunal

(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.

(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);

(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.

Appeals from Tribunal

100 (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(1);

(b) an order made under subsection 92(2); or

(c) a decision made under subsection 93(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(1) that sets out the finding, order or decision.

101 (1) A complainant or organization that is affected by an interim order made under paragraph 98(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.

Offenses and penalties

—**125** Every organization that knowingly contravenes section 58 (breach notification to OPC), subsection 60(1) (maintaining records of security breaches), section 69 (retention of information to allow individuals to exhaust recourse) or 75 (re-identification of information) or subsection 124(1) (whistleblowing) or an order under subsection 92(2) (breach of compliance order made by OPC) 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.

Private rights of action

106 (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(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(2) has expired, or

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

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

(2) If an organization has been convicted of an offence under section 125, 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.

Private rights of action

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.

Further reading

- McCarthy Tetrault lawyers, Canada's Privacy Overhaul: Deep Dive into Key Topics of Cross Border Transfers, Service Provider Obligations, AI, Employment Considerations and Class Action Developments
- McCarthy Tetrault lawyers, Canada's Privacy Overhaul: Deep Dive into the Key Topics of Data Subject Rights, Consent, De-identification, the Tribunal / Litigation and Data Governance
- Barry Sookman, CPPA: identifying the inscrutable meaning and policy behind the de-identifying provisions
- Barry Sookman, CPPA: transfers of personal information to service providers
- Dan Glover, Jade Buchanan, Kelsey Franks, CPPA: Welcome Clarification on Contractual and Other Duties on Cross-Border Transfers of Personal Information
- Barry Sookman, Liability under the CPPA
- Barry Sookman, Gillian Kerr, Nikiforos Iatrou, Pippa Leslie, The CPPA's Privacy Law Enforcement Regime
- Dana Siddle, Dan Glover, Colten Dennis, Consent Standards under the Proposed Consumer Privacy Protection Act
- Barry Sookman, Trade in Intangibles and impacts of the CPPA on small business
- Jade Buchanan, Dan Glover, Karine Jolzil, Charles Morgan, Michael Scherman,, Hello CPPA & PIDPT: The Federal Government Proposes Dramatic Evolution of PIPEDA
- Barry Sookman, Dan Glover, Jade Buchanan, Exceptions from consent in PIPEDA: facial recognition, privacy and Clearview

mccarthy tetrault

Slides first published on barrysookman.com @

https://wp.me/p3flp9-7Ak.

mccarthy tétrault

VANCOUVER

Suite 2400, 745 Thurlow Street
Vancouver BC V6E 0C5
Tel: 604-643-7100
Fax: 604-643-7900
Toll-Free: 1-877-244-7711

CALGARY

Suite 4000, 421 7th Avenue SW
Calgary AB T2P 4K9
Tel: 403-260-3500
Fax: 403-260-3501
Toll-Free: 1-877-244-7711

TORONTO

Suite 5300, TD Bank Tower
Box 48, 66 Wellington Street West
Toronto ON M5K 1E6
Tel: 416-362-1812
Fax: 416-868-0673
Toll-Free: 1-877-244-7711

MONTRÉAL

Suite 2500
1000 De La Gauchetière Street West
Montréal QC H3B 0A2
Tel: 514-397-4100
Fax: 514-875-6246
Toll-Free: 1-877-244-7711

QUÉBEC CITY

500, Grande Allée Est, 9e étage
Québec QC G1R 2J7
Tel: 418-521-3000
Fax: 418-521-3099
Toll-Free: 1-877-244-7711

NEW YORK

55 West 46th Street Suite 2804
New York NY 10036
UNITED STATES
Tel: 646-940-8970
Fax: 646-940-8972

LONDON

1 Angel Court, 18th Floor
London EC2R 7HJ
UNITED KINGDOM
Tel: +44 (0)20 7786 5700
Fax: +44 (0)20 7786 5702