Canada's Privacy Overhaul: Deep Dive into Key Topics

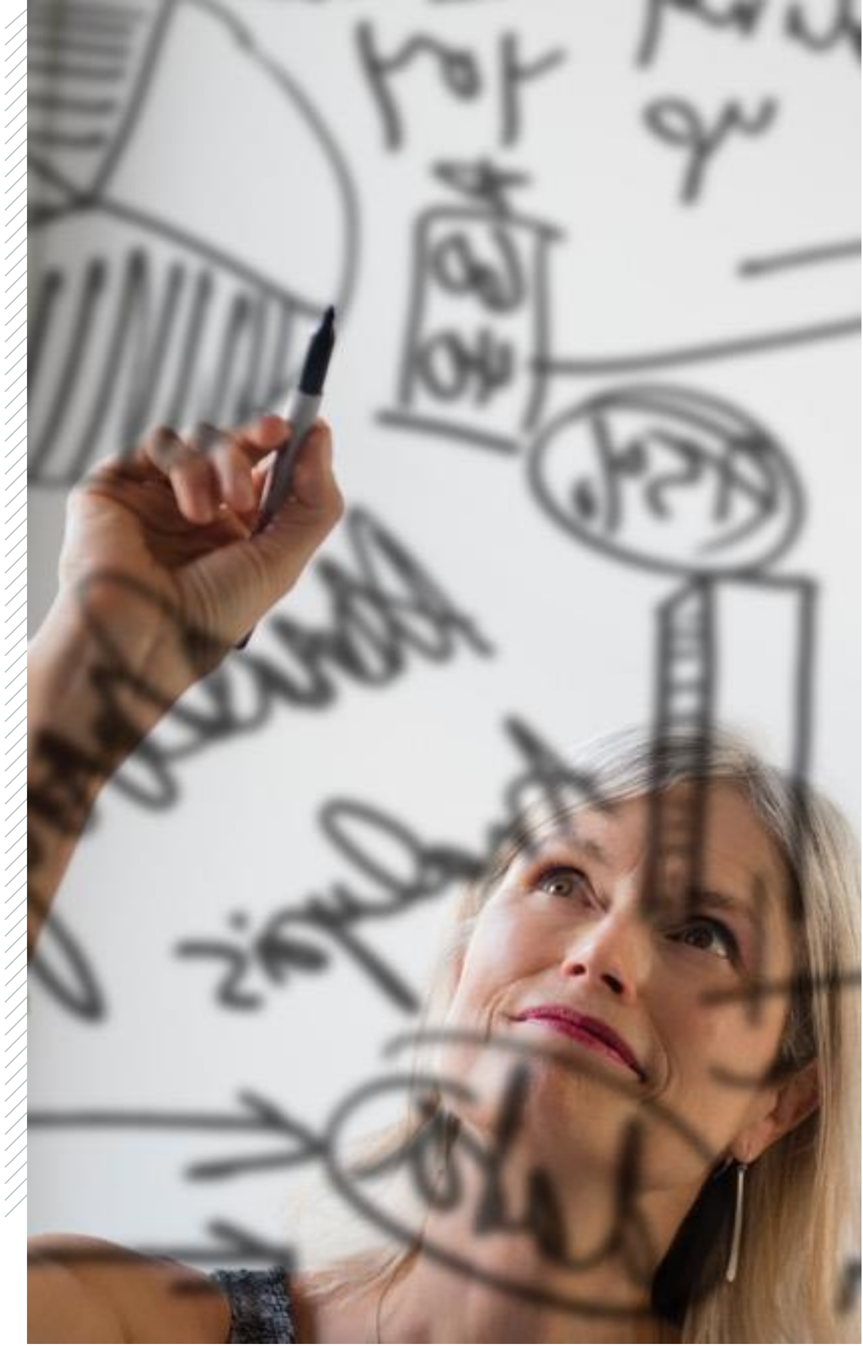
Part 1

February 24, 2021

mccarthy tetrault

Agenda

1. Introduction
2. New Data Subject Rights – Jade Buchanan
3. Consent and Consent Exceptions – Dan Glover
4. De-Identification – Barry Sookman
5. Tribunal / Litigation / Private Right of Action – Gillian Kerr and Karine Joizil
6. New Data Governance / Policies – Susan Wortzman
7. Questions



mccarthy tetrault

New Data Subject Rights

The Place of Consent in Privacy Law

Where are we now

—Consent described as the “**cornerstone**” of PIPEDA, *yet* commissioners admit that “**consent is simply not practicable in certain circumstances**” and ISED recognizing “**consent fatigue**”

—SCC in *Trang* recognizes implied consent available even for mortgage information *yet* commissioners applying *Guidelines for obtaining meaningful consent* with extreme vigour

- —Express consent for “**sensitive**” information, where handling is outside “**reasonable expectations**”, or where there is a “**meaningful residual risk of significant harm**” → easy for commissioners to demand express consent

—Commissioners read down exceptions to consent (*Clearview*)

—Consent awkward in “ecosystem of vast, complex information flows”

- —*Cadillac Fairview* requiring consent for a “few milliseconds” of processing

Where we're going

- CPPA **enlarges** and **clarifies** PIPEDA consent provisions *but* creates a modernized list of exceptions to the consent principle

- Consent *not* king: ss. 12-13 of CPPA emphasizes that purposes **must** be reasonable, minimal and effective:
  - For example, organizations must ask if there are "less intrusive means of achieving those purposes at a comparable cost and with comparable benefits"

- Consent requires **plain language, specific types** of PI, and **types of third parties** for disclosure (s. 15(3))

- **Onus** to prove appropriateness of implied consent (s. 15(4))

- But there are **powerful new exceptions,** including:
  - **"business activity" exception**, allowing collection for a closed set of purposes, including that it is "necessary to provide or deliver a product or service that the individual has requested" → narrower than GDPR Art. 6 "legitimate interests"
  - **"transfer to service provider" exception** → affirming cross-border guidelines
  - **"de-identification" exception** → helpful in theory, but kinks to be worked out

mccarthy tetrault

De-identification under the CPPA

What is de-identification and why is it important?

- Often used as a general term that includes privacy and security processes that renders personal information as either “anonymized” or “pseudonymized”.
- “Pseudonymization” a method that removes or replaces direct identifiers from a data set leaving in place data that could be used to indirectly identify a person with other data. This data is generally still subject to privacy laws.
- “Anonymization” a stronger form of de-identification which (depending on the formulation) makes re-identification impossible, reasonably unlikely, or not reasonably expected.
- Value of data; R&D, AI, big data, security etc

Is de-identified data subject to privacy laws?

– PIPEDA defines personal information as “information about an identifiable individual”. Thus, when information is “not about” an individual that can be identified, it is not personal information.

– “Information will be about an identifiable individual if there is a serious possibility that someone could identify the available information.” *PIPEDA Case Summary #2009-018*; *Gordon v. Canada (Health)*, 2008 FC 258.

– “an ‘identifiable’ individual is considered to be someone whom it is reasonable to expect can be identified from the information in issue when combined with information from sources otherwise available”. *Canada (Information Commissioner) v. Canadian Transportation Accident Investigation & Safety Board*, 2006 FCA 157.

Is de-identified data subject to privacy laws internationally?

- GDPR: “Personal data which have undergone pseudonymisation, which could be attributed to a natural person by the use of additional information should be considered to be information on an identifiable natural person. To determine whether a natural person is identifiable, account should be taken of all the means reasonably likely to be used, such as singling out, either by the controller or by another person to identify the natural person directly or indirectly. ..This Regulation does not therefore concern the processing of such anonymous information, including for statistical or research purposes” Recital 26
- CCPA: “*Deidentified”* means information that cannot reasonably identify, relate to, describe, be capable of being associated with, or be linked, directly or indirectly, to a particular consumer, provided that a business that uses deidentified information…”

mccarthy tetrault

CPPA amendments

- **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.
- This language suggests that no substantial change is intended by the law, but…..

Is de-identified information subject to the CPPA?

- Other amendments suggest de-identified data is subject to all CPPA obligations.
- **New exceptions for uses of de-identified data**
  - s. 21 for an organization’s internal research and development purposes
  - S.22. for a prospective business transaction
  - s.39 for a socially beneficial purpose
- **New standard for de-identification:** s.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.

Comments on CPPA amendments

- Ambiguous at best.
- A radical change from PIPEDA?
- Departure from the highest international privacy standards?
- Risks impeding uses of anonymized data?
- Impose heavy compliance costs that do not exist in the EU or the United States, even under the CCPA, including the fair information principles, e.g., consent, retention and disposal, limiting collection, service providers, security, openness.
- Impair the interoperability of our federal privacy law with provincial laws and with those of our major trading partners and undermine our competitiveness domestically and internationally?
- Needs fixing.

Further reading

- GDPR
- *California Consumer Privacy Act of 2018,*
- IPC *De-identification Guidelines for Structured Data*
- *Strengthening Privacy for the Digital Age*, ISED, *Proposals to modernize the Personal Information Protection and Electronic Documents Act*
- Department of Justice, *Greater certainty for Canadians and government: delineating the contours of the Privacy Act and defining important concepts*
- Irish Data Authority, *Guidance Note: Guidance on Anonymisation and Pseudonymisation* June 2019
- *See*, *Does anonymization or de-identification require consent under the GDPR?*
- Mike Hintze and Khaled El Emamet *Comparing the Benefits of Pseudonymization and Anonymization Under the GDPR*

mccarthy
tetrault

Tribunal Litigation Private Right of Action

mccarthy tetrault

New Data Governance & Policies

CPPA Data Governance Requirements

- CPPA Section 9(1) mandates a "privacy management program"
- Policies, practices and procedures must address:
  - protection of personal information
  - access requests and complaint procedures
  - training and internal information relating to policies, practices and procedures
  - development of external materials to explain the organization's policies and procedures
- In developing a privacy management program, organizations must take into account the volume and sensitivity of the personal information under its control. Therefore, the more you have, the more stringent the requirements. (Section 9(2))

CPPA Data Governance Requirements

- Sections 12(3) and (4) impose new record keeping obligations requiring companies to document the purposes for which personal information is collected, used or disclosed and to continually update if new purposes arise.
- Sections 13 and 14 limit organizations to collecting only necessary personal information, unless it is the subject of an exception.
- Section 57(1) and (2) mandates that organizations must protect personal information through physical, organizational, and technological security safeguards. This requires taking into account the quantity, distribution, format and method of storage of the information.
- Section 60 mandates the requirement to track security breaches involving personal information even if the brief did not meet a reporting threshold.

Practical Solutions for Managing Personal Information

- Implement an information governance strategy that includes the development of a privacy management program. This involves:
  - Know your data. How is personal information identified? Where is it stored? Who has access to it?
- Develop clear policies and procedures to manage the lifecycle of information from creation to storage or disposition.
- Create a data map that tracks where the information is stored.
- Leverage technology solutions to assist with the implementation of the policies.
- Train employees to manage and control personal information.

Questions?

mccarthy tetrault

Canada’s Privacy Overhaul: Deep Dive into Key Topics - Part 2

Wednesday March 3, 2021

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