Do you know what your neighbor is doing?

What US businesses need to know about the changing privacy landscape in Canada

April 28, 2021

Speakers

Peter Stockburger
Partner, San Diego
D +1 619 595 8018
Orange County
D +1 949 732 3707
peter.stockburger@dentons.com

Kirsten Thompson
National Lead of Transformative Technologies and Data Strategy Group
Partner, Toronto
D +1 416 863 4362
kirsten.thompson@dentons.com

Agenda

1. Overview: privacy landscape in Canada, and what is changing
2. The basics: overview of main provisions in the CPPA
3. Key issues for businesses:
   - Consent
   - De-identification
   - Service providers
   - Cross border transfers
4. So…what do I need to do?

Bill 64 in Quebec

1. Canada's privacy landscape…and what is changing

- **Currently:** *Personal Information Protection and Electronic Documents Act* ("**PIPEDA**")
  - 20 years old
  - Privacy + electronic document equivalency
  - "Principles based" and "technology neutral"
  - Privacy Commissioner = ombudsman role, not enforcement
  - determined to be "adequate" by EU Commission, but up for review (no later than 2022)

- **Proposed Bill C-11:** *Consumer Privacy Protection Act* ("**CPPA**")
  - Builds on PIPEDA, but divides PIPEDA into privacy (CPPA) and a separate piece of legislation for electronic documents
  - Still principles based, but codifies the principles
  - Privacy Commissioner = enforcement powers
  - Aligned with key concepts in the GDPR (and hopefully will be "adequate")

- What else? Quebec (**Bill 64**), British Columbia…and Ontario (?)

CPPA – why does it matter?

The federal Privacy Commissioner would be able to issue orders to organizations for privacy violations and recommend significant administrative penalties (AMPs), up to **3% of global turnover or $10M**, for a limited list of key infractions.

There are also offences based on another set of key infractions. These offences carry fines to a maximum of **5% global turnover or $25M**, whichever is highest.

Bonus: Private right of action.

Organizations should anticipate substantially higher compliance costs and consequences for non-compliance under the new regime.

The CPPA – when can we expect it?

Stage	Timing
Introduction	• November 17, 2020
2nd reading	• November 24, 2020…..April 19, 2021…
Referral to Committee	• Clause-by-clause review by parliamentary committee • Can summon witnesses and experts • Reports bill to the House, indicating amendments proposed. House considers amendments and votes for or against them
Third reading	• Debate and vote on bill as amended • Once bill has been read 3 times in the House, it is sent to the Senate for its consideration
Royal Assent	• Becomes law, but may/may not be "in force"
In Force	• Upon Royal Assent, when proclaimed, or on a day specified (12-18 month transition period expected)

Bill currently stalled in the House of Commons, creating risk that it will "die" on the Order Paper if Parliament is dissolved and an election is called later this year.

2. The basics: overview of main provisions in the CPPA

2. CPPA – the basics

Category	Specifics

Privacy program	• Privacy mgmt program required, plain language disclosures
	  • policies, practices and procedures (incl. protection of PI, requests for access to PI, training for staff, and explanatory materials)
	  • plain language required
	• Federal Office of the Privacy Commissioner of Canada (OPC) empowered to request to see an organization's privacy program

Purpose	• Appropriate purpose must consider specific "factors", be documented

2. CPPA – the basics

Category	Specifics
Consent	• Validity of consent contingent on certain info being provided to user • Express consent assumed; organization must demonstrate appropriateness otherwise • Refusal of withdrawals of consent now available for “reasonable terms of a contract”
Consent (exceptions)	• Additional exceptions to consent, including for certain “business activities” (marketing, etc. excluded)
Individual right	• Data mobility required
Transparency	• Disclosure of automated decision making (algorithmic transparency) • Right to request information

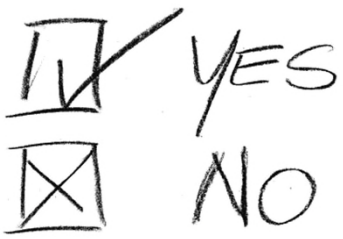
2. CPPA – the basics

Category	Specifics
Individual right	• Disposal (deletion) of personal information now required
Consent (exception - de-identification	• Certain uses of personal information, once de-identified, don’t require consent (including internal research activities)
Breach	• Expansive breach notification requirement for service providers to data controllers
Self-regulation	• Codes of practice, certification program
Enforcement	• new administrative Tribunal with privacy jurisdiction • OPC could issue orders • monetary penalties, fines

3. Impact on business

3. Impact on Business - Consent

- CPPA is still consent-based
- **Reverse onus:** presumption that **consent must be express (opt in)** – unless organization can demonstrate that implied consent is appropriate
- In coming to its conclusion about the **form of consent**, the organization must take into account "the reasonable expectations of the individual and the sensitivity of the personal information that is to be collected, used or disclosed."



3. Impact on Business - Consent

- Consent is not a get-out-of-jail-free card
- Even with consent, the **purpose** of collection must always be "reasonable"
- New "factors" that **must** be considered when trying to determine whether a purpose is reasonable:

  a. the **sensitivity** of the personal information;

  b. whether 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. Impact on Business - Consent

Good news: there are exceptions to consent

Under the CPPA, knowledge and consent would not be required for:

1. Business activities
   - Organizations could collect or use (but not disclose) PI without knowledge or consent if the collection or use is for a listed "business activity"* (described further below) **and**:
     - a reasonable person would expect such a collection/use for that activity; **and**
     - **the PI is not collected or used for the purpose of influencing the individual's behaviour or decisions**
2. Transfers to service providers
3. De-identification, and certain uses of de-identified information

* *A Business activity: an activity which is (a) **necessary to provide or deliver a product or service** that the individual has requested from the organization; (b) carried out in the exercise of **due diligence** to prevent or reduce the organization's commercial risk; (c) **necessary for the organization's information, system or network security**; (d) **necessary for the safety of a product or service** that the organization provides or delivers; or (e) for which **obtaining consent would be impracticable** because the organization has no direct relationship with the individual.*

3. Impact on Business - Consent

Bad news: the exceptions don't cover many activities important to business

- This includes where **the personal information is collected or used for the purpose of influencing the individual's behaviour or decisions**
- What counts as influencing behaviour or decisions?
  - Arguably, any collection or use of personal information for marketing – which would include profiling and targeted ads
- Consent would still be required – and the business would have to determine whether consent should be express or implied
  - Good news: in most cases, implied consent would likely be sufficient
  - However, individuals have a right to withdraw their consent and/or demand disposal/deletion of their personal information – organizations will need to be able to manage this

3. Impact on Business – De-identified information

- 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"

Good news: can use de-identified information without knowledge or consent for internal research and development

Bad news:

- De-identified personal information – ***even if completely anonymized*** – is still caught by the CPPA
- Information created from personal information – ***even if not identifying*** – is caught by the CPPA

3. Impact on Business – 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
- PI 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 PI is collected, used or disclosed by the organization itself or by a service provider on behalf of the organization
  - Controller must ensure that service provider provides **substantially the same protection**
  - Service provider can only use PI for controller's purpose – not its own

Good news – main CPPA obligations do not apply to service providers re transferred PI. However, if the service provider collects, uses or discloses that information for any other purpose, the CPPA applies as if it were a controller

3. Impact on Business – Cross border transfers

Good news: No change here – formalization of *status quo*

- Contrary to Québec Bill 64 and the GDPR, which provide for an evaluation of the foreign privacy framework's level of equivalency, but in line with PIPEDA and past guidance from the OPC, the CPPA **does not contain any restriction to the transfer of personal information outside of Canada**
- However, there is a **transparency obligation**:
  - The organization's privacy policy must include details as to whether the organization carries on any international or interprovincial transfer or disclosure of personal data…. but only "to the extent such transfer or disclosure may have reasonably foreseeable privacy implications."
  - Unclear - seems to imply that this information must only be included where personal information is shared with an organization/entity that may not protect it adequately or may be subject to laws that are not substantially similar to the CPPA

4. So…what do I need to do?

4. So….what do I need to do?

CPPA provision	What companies need to do
Privacy mgmt program required, plain language disclosures • Policies, practices and procedures (incl. protection of PI, requests for access to PI, training for staff, and explanatory materials)	Review existing materials and practices and close gaps, rewrite
Appropriate purpose must consider "factors", be documented	Review "purposes" of all collection in accordance with factors, and document
Validity of consent contingent on certain info being provided to user	Review all documents used to obtain consent to ensure appropriate disclosures being made
Express consent assumed	Onus on organization to establish implied consent appropriate

4. So….what do I need to do?

CPPA provision	What companies need to do
Refusal of withdrawals of consent now available for "reasonable terms of a contract"	Review and revise contracts to include specific terms where necessary
Additional exceptions to consent	Undertake data mapping and consent tracking to determine available exceptions, ensure criteria met
Data mobility required	Inventory qualifying information and ensure process for transfers
Algorithmic transparency	Assess whether automated decision-making is being used (vendors?), develop plain language
Disposal of personal information	Development documented processes, incl. for service providers, and in response to requests

4. So….what do I need to do?

CPPA provision	What companies need to do
De-identification requirements and restrictions	Review de-identification processes, understand criteria, document & apply
Expansive breach notification requirement for service providers to data controllers	Develop process for reporting, handling
Codes of practice, certification programs	Details pending in expected regulations

Quebec: Bill 64

- Enhanced consent for public and private sector. Must be:
  - Free and informed, and given for specific purposes;
  - **Requested for each purpose**, and **separately from any other information**;
  - Not obtained from individuals under 14; and
  - Express when it concerns sensitive personal information.
- Before sending personal information outside Quebec (incl. to another province), a privacy impact assessment must be done that evaluates:
  - The sensitivity of the information;
  - The purposes for which it is to be used;
  - The protection measures which would apply to it; and
  - **The legal framework of the State where the information would be released**, including its degree of equivalency with the personal information principles applicable in Quebec.

Thank you

Dentons is the world's largest law firm, connecting talent to the world's challenges and opportunities in more than 75 countries. Dentons' legal and business solutions benefit from deep roots in our communities and award-winning advancements in client service, including Nextlaw, Dentons' innovation and strategic advisory services. Dentons' polycentric and purpose-driven approach, commitment to inclusion and diversity, and world-class talent challenge the status quo to advance client and community interests in he New Dynamic.

dentons.com