

# Modernization of Canadian Privacy Law: Where are we heading?

Scott Lamb, Partner – Clark Wilson LLP  
Jeff Holowaychuk, Associate – Clark Wilson LLP  
Marc Yu, Partner – Field Law  
Richard Stobbe, Lawyer, Trademark Agent, CLP – Field Law

CLARK WILSON LLP | **FIELD LAW**

---

---

---

---

---

---

---

---

## 1. Introduction

CLARK WILSON LLP | **FIELD LAW**

---

---

---

---

---

---

---

---

## 2. Background

CLARK WILSON LLP | **FIELD LAW**

---

---

---

---

---

---

---

---

## Background

1970s - the office of the Privacy Commissioner of Canada

**PIPEDA (2000) – CSA Model Code**

- Federal application
- Private sector
- "substantially similar": Alberta, B.C. and Quebec

CLARK WILSON LLP | FIELD LAW

---

---

---

---

---

---

---

---

## Background (cont'd)

- Health sector legislation in Canada
- Private sector privacy laws: BC, AB and Quebec
- Privacy maturity – impetus through GDPR, California and Quebec
- Federal analysis of privacy reform (20 yrs since PIPEDA)

CLARK WILSON LLP | FIELD LAW

---

---

---

---

---

---

---

---

## 3. New Federal Legislation CPPA and Tribunal Act

CLARK WILSON LLP | FIELD LAW

---

---

---

---

---

---

---

---

## New Federal Privacy Legislation

### Digital Charter Implementation, 2020

Creates two new pieces of legislation:

- Consumer Privacy Protection Act
- Personal Information and Data Protection Tribunal Act

**Current Status:** In-depth review by parliamentary committee

---

---

---

---

---

---

---

---

---

---

## 4. Collection, Use and Disclosure – Consent Issues and Exceptions

---

---

---

---

---

---

---

---

---

---

## Collection, Use and Disclosure

Meaningful/valid consent issues (Section 15)

In plain language

- Why - the **purposes** for the collection, use or disclosure
- How - the **way** in which the personal information is to be collected, used or disclosed
- What – the **specific type** of personal information that is to be collected, used or disclosed
- Who – the **names or types** of third parties to which the organization may disclose the personal information
- Any reasonably foreseeable **consequences** of the collection, use of disclosure of the personal information

---

---

---

---

---

---

---

---

---

---

## Express Consent

Express Consent: express (versus implied) consent is now the default

Section 15 (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."

- Compare CSA Model Code: "...an organization should generally seek express consent when the information is likely to be considered sensitive. Implied consent would generally be appropriate when the information is less sensitive

---

---

---

---

---

---

---

---

---

---

## Withdrawal of Consent

Withdrawal of Consent: Section 17  
Consequences of withdrawal

- Compare: CSA Model Code 4.3.8

---

---

---

---

---

---

---

---

---

---

## Exceptions to Consent

Consent exceptions: Section 18

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 **specific business activity 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.

---

---

---

---

---

---

---

---

---

---

### Exceptions to Consent

Consent exceptions: Section 18 (**specific business activities**)

- an activity that is **necessary to provide or deliver a product or service** that the individual has requested from the organization;
- an activity that is carried out in the exercise of **due diligence** to prevent or reduce the organization's commercial risk;
- an activity that is necessary for the organization's **information, system or network security**;
- an activity that is necessary for the **safety of a product or service** that the organization provides or delivers;
- 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.

CLARK WILSON LLP | FIELD LAW 13

---

---

---

---

---

---

---

---

## 5. De-Identification and Research

CLARK WILSON LLP | FIELD LAW 14

---

---

---

---

---

---

---

---

### De-Identification and Research

- Canadian competitiveness
- Current state of anonymization under PIPEDA
- GDPR and Californian law

CLARK WILSON LLP | FIELD LAW 15

---

---

---

---

---

---

---

---

**De-Identification and Research (cont'd)**

- CPPA reform
  - Definition of "de-identify" (s.2)
  - Whether consent required to de-identify (s. 20)
  - Prohibition to re-identify (s.75)

CLARK WILSON LLP | FIELD LAW 16

---

---

---

---

---

---

---

---

**De-Identification and Research (cont'd)**

- CPPA reform
  - Proportionality of technical and administrative measures (s. 74)
  - Use for research and development (s. 21)
  - Disclosure for socially beneficial purposes (s. 39)
  - Use and disclosure for prospective business transaction (s. 22)

CLARK WILSON LLP | FIELD LAW 17

---

---

---

---

---

---

---

---

**6. New "Rights" Under CPPA**

CLARK WILSON LLP | FIELD LAW 18

---

---

---

---

---

---

---

---

## New "Rights" Under CPPA

### Right to Erasure

- Right to require organizations to delete data
- Disposal at individual's request

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.

- Social media implications

---

---

---

---

---

---

---

---

---

---

## New "Rights" Under CPPA (cont'd)

### Mobility / Data Portability

- Individual right to transfer data from one organization to another
- "data mobility frameworks" to be approved by regulation as secure mechanisms for enabling mobility

---

---

---

---

---

---

---

---

---

---

## New "Rights" Under CPPA (cont'd)

### Private Right of Action (Section 106) Damages

(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 that the organization has contravened this Act
- (b) the Tribunal has made a finding that the organization has contravened this Act.

---

---

---

---

---

---

---

---

---

---

### New "Rights" Under CPPA (cont'd)

(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.**

- Section 58 (breach notification),
- Section 60(1) (maintain records of a security breach),
- Section 69 (retention of information) or
- Section 75 (prohibition against using de-identified information)
- Section 124(1) (whistleblower protection)
- or an order under subsection 92(2) or obstruction of the Commissioner in the investigation of a complaint

---

---

---

---

---

---

---

---

---

---

## 7. Outsourcing

---

---

---

---

---

---

---

---

---

---

## Outsourcing

### Accountability

- An organization is accountable for personal information in its control
- New Definition of "control" - "Personal information "is under the control of the organization that decides to collect it and that determines the purposes for its collection, use and disclosure."
- Accountability remains if personal information is transferred to a service provider for processing
- Must ensure that the service provider protects that personal information in substantially the same manner

---

---

---

---

---

---

---

---

---

---



## Outsourcing (cont'd)

### Transfers to Service Providers

- A transfer of personal information to a service provider does not require the consent of or notice to the individual
- No requirement to obtain consent to transfers or processing outside of Canada, but notice might be required in some circumstances

### Disposal

- After receiving a request for disposal, organization must obtain confirmation from a service provider that information has been disposed of.

---

---

---

---

---

---

---

---

---

---

## Outsourcing (cont'd)

### Service Provider Obligations

- More clarity around role of service providers
- Not responsible for complying with Part 1 other than:
  - **Section 57** – Appropriate physical, organizational and technological security safeguards
  - **Section 61** – Notify customer of any breach of security safeguards that involves personal information
- Secondary uses (using personal information for other purposes)

---

---

---

---

---

---

---

---

---

---

## 8. Enforcement

---

---

---

---

---

---

---

---

---

---

## Enforcement

- PIPEDA shortcomings
- CPPA new powers for Privacy Commissioner
  - Compliance Orders (s. 92(2))
  - Recommend penalties
    - Factors for making recommendations (s. 93)
      - » Nature and scope of breach
      - » Whether voluntarily paid compensation to person affected
      - » History of compliance
      - » Other relevant factors

---

---

---

---

---

---

---

---

## Enforcement (cont'd)

- New Data Protection Tribunal
  - Exclusive power to impose penalties (s. 94)
  - Maximum penalties
- Higher of \$10 million or 3% of gross global revenue (s. 94(4))
  - Factors for imposition of penalties (s. 94(5))
    - » Factors listed for Privacy Commissioners recommendation
    - » Organizations ability to pay and ability to carry on business
    - » Benefit the organization obtained from the breach
  - Stated "purpose of penalties not to punish but to promote compliance" (s. 94(6))
  - Tribunal cannot impose penalties if prosecution for breach instituted or if the organization establishes due diligence (s. 94(3))

---

---

---

---

---

---

---

---

## Enforcement (cont'd)

- Fines imposed if breach of certain provisions of CPPA (s. 125)
  - Failure to report data breaches
  - Failure to keep and maintain records of data breaches
  - Failure to retain personal information that is subject to access request
  - Using de-identified personal information to identify an individual
  - Obstruct the Privacy Commissioner

---

---

---

---

---

---

---

---

## Enforcement (cont'd)

- Fines imposed in prosecution by Attorney General of Canada (not new Data Protection Tribunal)
- Maximum fines (s. 125)
  - Indictable offences
    - » Higher of \$25 million or 5% of gross global revenue
  - Summary offences
    - » Higher of \$20 million or 4% of gross global revenue

---

---

---

---

---

---

---

---

## 9. Privacy Management Programs

---

---

---

---

---

---

---

---

## Privacy Management Programs

- CPPA requires every organization to implement a PMP that includes policies, practices, and procedures respecting:
  - Protection of personal information
  - How access requests and complaints will be handled
  - Training and information provided to staff
  - Development of materials to explain policies and procedures

---

---

---

---

---

---

---

---

### Privacy Management Programs (cont'd)

- Organization must take into account the volume and sensitivity of the personal information under its control.
- Commissioner may seek access to policies, practices, and procedures.
- Similar to PIPEDA Principle 4.1.4

---

---

---

---

---

---

---

---

### Privacy Management Programs (cont'd)

- Recommendations from Alberta IPC
- Requirement for organizations to have privacy management program proportionate to its size and volume/sensitivity of personal information.
  - Direct response to GDPR, Quebec's Bill 64 and the CPPA.

---

---

---

---

---

---

---

---

### Privacy Management Programs (cont'd)

- "Technical and organizational measures to ensure that organizations plan ahead and build privacy into new products and services".
- Written information available to public, PIAs, automated decision-making notification and rights to object.

---

---

---

---

---

---

---

---

**Privacy Management Programs (cont'd)**

- Privacy policy and procedures
  - E.g. Website policy/cookie policy, breach response procedures
- Designation of roles within organization
  - Privacy Officer/Data Protection Officer
  - Senior management
  - Employees

CLARK WILSON LLP | FIELD LAW 37

---

---

---

---

---

---

---

---

**Privacy Management Programs (cont'd)**

- Development of organizational practices
  - Data inventory mapping
  - Privacy audit- internal or third party
  - Management of third party service providers
- Maintenance of PMP/Continuing Education
  - Amendments to legislation
  - Advisories from regulatory bodies

CLARK WILSON LLP | FIELD LAW 38

---

---

---

---

---

---

---

---

**10. Alberta Update**

---

CLARK WILSON LLP | FIELD LAW 39

---

---

---

---

---

---

---

---

## Alberta Update

- Privacy Impact Assessments
  - Currently required under the Alberta Health Information Act (HIA).
  - Commissioner recommends requiring public bodies to complete privacy assessments for information sharing initiatives, when developing an information system or an electronic service delivery project, or where they plan to disclose personal information without consent, or disclose personal information outside of the province.

---

---

---

---

---

---

---

---

## Alberta Update (cont'd)

- PIA Challenges
  - Significant backlog in PIA review with OIPC.
  - 1,454 opened and 1,071 closed PIAs in 2019-2020 in Alberta.
  - What should organization or public bodies do when PIA acceptance is "pending"?

---

---

---

---

---

---

---

---

## Alberta Update (cont'd)

- Individual rights and data portability (PIPA)
- Increased scope of PIPA- non-profit organizations and political parties
- Breach reporting (FOIPPA)
  - Required under Alberta's HIA and PIPA.
  - Recommendation that FOIPPA be amended to include breach reporting.
  - Threshold - "real risk of significant harm".

---

---

---

---

---

---

---

---

### Alberta Update (cont'd)

- Access and Solicitor Client Privilege
- Recommendation that public bodies be compelled to provide records to Commissioner where claims of privilege are being reviewed.
- Recent Alberta decisions on access and SCP:
  - *Edmonton Police Service v. Alberta (Information and Privacy Commissioner)*, 2020 ABQB 10
  - *Alberta Health Services v. Farkas*, 2020 ABQB 281

CLARK WILSON LLP | FIELD LAW 43

---

---

---

---

---

---

---

---

### Alberta Update (cont'd)

- Rule of law demands that people are able to seek appropriate legal assistance.
- Corporations and public bodies are equally entitled to legal counsel (in-house legal departments) and privilege like individuals.
- Privilege should not be assessed by isolating particular communications or fragments of communications.
- Scope of privilege applies to a "continuum" - not just the culmination of the lawyer's product or opinion.

CLARK WILSON LLP | FIELD LAW 44

---

---

---

---

---

---

---

---

### 11. BC Update

---

CLARK WILSON LLP | FIELD LAW 45

---

---

---

---

---

---

---

---

### Review of BC's Personal Information Protection Act

- Review of PIPA is required every 6 years.
  - Special Committee appointed in 2020
  - Public consultations conducted in Summer 2020
  - Report with recommendations for changes was to be tabled in the Legislative Assembly in February 2021

CLARK WILSON | FIELD LAW 46

---

---

---

---

---

---

---

---

### Review of BC's Personal Information Protection Act

#### Likely Recommendations for Change

- Mandatory Breach Notification
- Enhanced oversight and enforcement powers
- Administrative Monetary Penalties
- De-identification
- PIAs

CLARK WILSON | FIELD LAW 47

---

---

---

---

---

---

---

---

### Review of BC's Personal Information Protection Act

#### Likely Recommendations for Change

- Clarifying consent requirements
- Additional grounds for processing without consent
- Additional individual rights
- Automated decision-making
- Clarity for outsourcing arrangements

CLARK WILSON | FIELD LAW 48

---

---

---

---

---





---

---

---



**QUESTIONS?**

|  |   |
|--|---|
|  <p><b>Scott Lamb</b><br/>Clark Wilson   Partner<br/>slamb@cwilson.com<br/>604 643 3103</p> |  <p><b>Jeff Holowaychuk</b><br/>Clark Wilson   Associate<br/>jholowaychuk@cwilson.com<br/>604 643 3194</p>           |
|  <p><b>Marc Yu</b><br/>Field Law   Partner<br/>myu@fieldlaw.com<br/>780 643 8767</p>        |  <p><b>Richard Stobbe</b><br/>Field Law   Lawyer, Trademark Agent, CLP<br/>rstobbe@fieldlaw.com<br/>403 260 8508</p> |

These materials are necessarily of a general nature and do not take into consideration any specific matter, client or fact pattern

CLARK WILSON LLP | FIELD LAW

---

---

---

---

---

---

---

---