Canadian Federal Privacy Law Reform:

Overview and Insights on Bill C-36's Proposed New Private Sector Privacy Regime

Special Monthly Privacy Call - June 19, 2026

Presented by the Partners of Osler's national Privacy and Data Management practice

ACCESSPRIVACY BY OSLER

Presentation Overview

- Legislative Reform Timeline
- Key Features of Legislative Reform Proposal
- New Regulatory Model
- Enforcement
- Application of the PPCDA
- Legislative Intent and Purpose
- Reasonable and Appropriate Provision
- Purpose Identification and Data Minimization
- De-Identification & Anonymization
- Accountability Provisions
- Concept of Service Provider
- Transfers/Disclosures Outside of Canada
- Codes of Practice/Certifications
- Children's Personal Information
- Consent Requirements
- Exceptions to Consent
- Transparency and Openness
- Automated Decision Systems
- Breaches of Security Safeguards
- Right of Disposal/Deletion
- Right of Data Mobility

Federal Private Sector Privacy Legislative Reform Timeline

April 2000: PIPEDA Receives Royal Assent

PIPEDA receives Royal Assent, with a mandatory parliamentary review every five years after Part I came into force (January 1, 2001) (s. 29(1)).

May 2019: Canada's Digital Charter Launched

Government of Canada launches Canada's Digital Charter and announces an initial set of actions to implement the Charter's principles, highlighted by proposals to modernize PIPEDA.

August 2021: Bill C-11 Dies on the Order Paper

Bill C-11 dies on the order paper at second reading when the legislative session is dissolved for the federal election.

January 2025: Bill C-27 Dies on the Order Paper

Bill C-27 dies on the order paper when Parliament is prorogued and later dissolved for the federal election.

November 2018: Digital Privacy Act Amendments in Force

Digital Privacy Act amendments to PIPEDA come into force, including the security breach notification regime.

November 2020: Bill C-11 Tabled

Bill C-11 is tabled in federal Parliament.

June 2022: Bill C-27 Tabled

Bill C-27 is tabled; in November 2022, the Speaker rules to separate the vote on the Artificial Intelligence and Data Act from Parts I and II (the Consumer Privacy Protection Act and the Personal Information and Data Protection Tribunal Act).

June 2026: Bill C-36 Tabled

Bill C-36 is tabled in federal Parliament.

Key Features of New Privacy Legislative Reform Proposal: The PPCDA

Similar to PIPEDA, the PPCDA's proposed statutory framework is grounded in:

- a balancing of the interests of individuals and organizations;
- a consent-based regime;
- rules generally drafted in principles-based, risk-calibrated, technologically neutral fashion; and
- an accountability model.

The PPCDA would introduce the following new features:

- An **enforcement regime** with potentially severe financial penalties and fines, a private right of action, and order-making power for the regulatory authority;
- Clarifications and additional **"exceptions to consent"** authorities for use and disclosures of personal information, including for standard "business activities" and for processing of personal information for "legitimate interests" (subject to strict requirements);
- Provisions relating to **"de-identified" and "anonymized" information**, and clarification the latter is not governed by the statute;
- Strengthened and more prescriptive **accountability requirements**;
- Clarification of the obligations of **service providers**;
- Requirement to implement and maintain a **privacy management program**;
- Statutory recognition of **"codes of practice" and certification** programs;
- New **data subject rights**: right of deletion, data portability right (the latter was added to PIPEDA via Bill C-15 but is not yet in force); and
- Transparency provisions regarding **automated decision systems**.

Key Features of New Privacy Legislative Reform Proposal – Updates from the CPPA

The proposed PPCDA is substantially similar to the statutory framework within former Bill C-27. Key updates include:

- Transferring authority for overseeing and enforcing the private sector privacy framework to the new **Digital Safety and Data Protection Commission of Canada** (also responsible for digital safety oversight under Bill C-34);
  - No accompanying standalone **legislation regulating AI**
  - **No standalone adjudicative tribunal** to enforce the PPCDA
  - Still **no comprehensive privacy protection** for personal information in the custody of **federal political parties** within the PPCDA (or any other statutory regime)

- Clarifying that the definition of "personal information" includes information **inferred** about the [identifiable] individual;

- Enhanced focus on **children's personal information:** new definition of a "child", contemplating children's personal information under the definition of "sensitive", and the explicit requirement for the Commission to take into account the "best interests of children";

- The ability to **disclose** (in addition to collect and use) an individual's personal information under the **legitimate interests** exception to consent;

- The requirement to conduct a **privacy impact assessment** and implement mitigating measures identified in the PIA prior to **disclosing/transferring personal information outside of Canada**;

- The opportunity for individuals to make **written representations** contesting an organization's decision made by an **automated decision system.**

Canadian Federal Privacy Law Reform: Overview and Insights on Bill C-36's Proposed New Private Sector Privacy Regime

Digital Safety and Data Protection Commission of Canada (Commission)

- Replaces the Office of the Privacy Commissioner of Canada for private sector privacy law regime.
- Overall oversight and enforcement of the PPCDA regime.
- Commission also administers the recently proposed Digital Safety Act (Bill C-34), which sets out a framework to govern online safety, reduce harms resulting from online content and establishes transparency and accountability requirements for operators of regulated services such as social media sites, chatbots and other online services.

Privacy and Consumer Data Commissioner (Commissioner)

Member of Commission · Investigative arm

- Unlike under PIPEDA, the Commissioner is not an independent agent of Parliament
- Investigation of complaints and self-initiated (ss. 97-100)
- Compliance agreements (in course of resolving investigations) (ss. 102-103)
- Notices of Contravention (ss. 105-108) — must include grounds for contravention, including the provisions of PPCDA that have been contravened, any penalty or "proposed order," and information regarding right to apply for a review.
  - If uncontested, deemed contravention and penalty is levied and "proposed order" is deemed to be made by Commission.
  - Injunctive relief (application for review to Commission) (s. 109)
  - Discretion to publish information where it is in public interest (s. 135(3))
- Audit/Investigation powers (ss. 118, 122)
- Ensures compliance with approved certification programs (s. 85)
- Above processes governed by guidance that will be developed by Commission in consultation with Minister and other stakeholders (s. 78)

Adjudicative Function of Commission

Excludes Commissioner & any member with reasonable apprehension of bias (ss. 111, 124)

- Hears applications for review of notices of contravention and interim orders issued by Commissioner (ss. 109, 123)
- Reviews, confirms, and varies penalties (s. 110)
- Reviews, confirms or varies proposed orders included in notices of contravention issued by Commissioner, and makes order (s. 110)
- Issuance of interim orders (s. 121)
- Must conduct in accordance with rules published by Commission (s. 78)

Commissioner cannot adjudicate (s. 111)

Federal Court

- Unlike PIPEDA, organizations can appeal decisions by Commission (ss. 126-128)

Privacy and Consumer Data Division (Division)

Commissioner & 1+ members of Commission

- Dispute Resolution to resolve complaints (s. 101)
- Approves codes of practice and certification programs (s. 93 -96)
- May be delegated a majority of Commission responsibilities, including developing guidance, conducting research and consultation with international stakeholders relating to compliance with Act.
  - Minister may request guidance materials, tools and research be conducted (s. 76)

New Enforcement Regime – Administrative Monetary Penalties

- Maximum AMP of the **higher of** $10 million or 3% of gross global revenues (s. 114)
- AMPs may only be imposed by Commission for **enumerated contraventions** (s. 113(1)), including:
  - Failing to implement and maintain a **privacy management program** (s. 9(1))
  - Failing to ensure an equivalent level of protection for personal information transferred to **service providers** (s. 11(1))
  - Failing to collect/use/disclose personal information for **reasonable and appropriate purposes** (s. 12(1))*
  - Failing to **determine the purpose** for collecting/using/disclosing personal information and **recording** those purposes and any new purpose before collection (s. 12(3) and 12(4))
  - Collecting personal information **beyond what is necessary** for purposes identified and recorded by an organization (s. 13)
  - Using or disclosing personal information for a **secondary purpose without consent**, unless an exception to consent applies (s. 14(1))
  - Failing to obtain **valid consent** (s. 15(1))

** Enumerated contravention not contained in former C-27*

New Enforcement Regime – Administrative Monetary Penalties

- AMPs may only be imposed by Commission for **enumerated contraventions** (s. 113(1)), including *[cont'd]:*
  - Contravening the **"refusal to deal"** provision (s. 15(7))
  - Obtaining consent through **false or misleading** information, or using **deceptive** practices (s. 16)
  - Failing to **inform** an individual of the consequences of **withdrawing their consent** and ceasing the collection, use or disclosure of their information in respect of which the consent was withdrawn (s. 17(2))
  - Contravening the **retention and disposal** requirements (s. 52, s. 54(1) and 54(5))
  - Contravening the **safeguarding** requirements (s. 56(1))
  - **Failing to report** a breach of security safeguards (s. 58(1))
  - **Failing to notify** affected individuals of a breach of security safeguards (s. 58(3))
  - A **service provider failing to notify** the organization of a breach of security safeguards (s. 61)
  - Failing to make **information regarding an organization's policies and practices** available (s. 62(1))

Process – Administrative Monetary Penalties

- Factors to be considered by Commissioner and Commission in determining the amount of an AMP (s. 113(2)):
  - **nature and scope** of contravention;
  - evidence of exercise of **due diligence** to avoid contravention;
  - whether the organization made **reasonable efforts** to **mitigate or reverse** the effects of contravention;
  - **history** of compliance;
  - the organization's **ability to pay** the penalty and the likely effect that paying it would have on the organization's ability to carry on its business*;
  - Any **financial benefit** that the organization obtained from the contravention*; and
  - any other **prescribed or relevant** factor
- Commissioner determines penalties after investigation (s. 109)
- Commissioner's decision to impose or ***not* to impose** monetary penalties (or any other determination) may be appealed by complainant or organization to Commission for review. (s. 109)
- After review, Commission can vary penalty (s. 110)

** Enumerated factors not contained in former C-27*

New Enforcement Regime – Offences & Fines

- Certain ***knowing*** contraventions may be prosecuted as offences in court and subject to **fines:**
  - Fines on conviction of an indictable offence may be up to higher of $25 million or 5% (s. 145(a))
  - Fines on conviction of a summary offence may be up to higher of $20 million or 4% (s. 145(b))
- Offences include:
  - failing to **report breach of security safeguards** or **notify affected individuals** (s. 58)
  - failing to provide Commission with **access to breach records** (s. 60(1))
  - failing to **retain personal information** that is subject of personal information request (s. 69)
  - using **de-identified personal information** to identify an individual in an unauthorized manner (s. 75)
  - retaliating against a **whistleblower** (s. 144(1))
  - contravening an **order made by the Commission** to ensure compliance with the PPCDA (s. 110(1))
  - **obstructing** an investigation, audit, or proceedings undertaken by the Commission/Commissioner (s. 109 and 123(4))

New Enforcement Regime – Private Right of Action & Order-Making Powers

- Order-making powers
  - Following an investigation, the Commission may **order an organization to comply and to publicize corrective measures** (s. 110))
  - In exigent circumstances, in carrying out an investigation or audit, the Commissioner may issue a notice of proposed interim order (s. 122)
  - During a review under s. 109 or 123, the Commission may make any **interim order** considered appropriate (s. 121(1)) and may make **information preservation orders** (s. 121(2)(d))
  - Compliance orders and penalties issued by the Commission **may be appealed** to the Federal Court (s. 126)
  - Interim orders may be appealed to Federal Court, but only with leave (s. 127(1))

- Private right of action. (s. 132)
  - After a final finding of contravention, the entering of a compliance agreement, or a conviction, affected individuals may sue for "**damages for loss or injury...suffered as a result**" (ss. 132(1) and (2))
  - Claims may be brought in either Federal Court or superior courts of provinces (s. 132(5))
  - Two-year limitation period running from final finding or conviction after all appeal rights have been exhausted (s. 132(4))

Application of the PPCDA

- Like PIPEDA, the PPCDA applies to the collection, use and disclosure of personal information in the course of commercial activities
  - Nature and scope of concept of "personal information" - "information about an identifiable individual, including information that is inferred* about the individual." (s. 2(1)), and includes:
    - sensitive personal information
      - "personal information in respect of which, taking into account the circumstances, an individual has a heightened expectation of privacy, including, as the case may be, a child's personal information, personal information revealing an individual's racial or ethnic origin, political opinions or religious or philosophical beliefs, an individual's trade union membership, genetic information or health information, biometric information that is capable of uniquely identifying the individual or information concerning an individual's sexual orientation" (s. 2(1))
    - de-identified personal information
      - personal information that has been modified "so that an individual cannot be directly identified from it, although a risk of the individual being identified remains" (s. 2(1))

**express reference to Inferred information not contained in former C-27's definition of personal information*

Application of the PPCDA

- The PPCDA does not apply to:
  - Collection, use, and disclosure outside the scope of an organization's commercial activities
    - C-36 reverts to PIPEDA's definition of "commercial activity", meaning "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" (s. 2(1))
  - "Anonymized" information
    - Information generated from personal information that has been "irreversibly and permanently [modified] to ensure that there is no reasonably foreseeable risk in the circumstances that an individual can be identified from the information, whether directly or indirectly, by any means" (ss. 2(1) and 6(5))
    - Note that anonymization may be subject to regulations (s. 139(1)(a))
  - Other circumstances as currently the case in PIPEDA, such as:
    - Collection, use or disclosure of personal information for personal or journalistic, artistic or literary purposes (ss. 6(4)(b) and (c))
    - Employee personal information in the context of provincially regulated employment relationships

Legislative Intent

- No preamble in the PPCDA (as compared to the lengthy preamble in C-27)
- Key change from Bill C-27 in the balanced "purpose" clause: express reference to privacy as a fundamental right
  - The purpose of this Act is to establish — in an era in which 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 protection of personal information in a manner that recognizes the **fundamental 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. (s. 5)

- In addition to the purpose of the Act (s. 5), the Commission, Commissioner and Division must take into account **all relevant factors** when exercising powers or performing duties or functions under the PPCDA (ss. 77, 86, 90). **Factors include, as applicable:**
  - the size and revenue of organizations;
  - the volume of the personal information under the control of organizations and the sensitivity of that information;
  - the best interests of children;
  - the importance of respecting Canada's international trade obligations;
  - the importance of supporting economic growth, competition and innovation in the Canadian marketplace; and
  - any other matter of general public interest.

Reasonable & Appropriate Provision

- The PPCDA (Section 12(1)) sets out the overarching "reasonable and appropriate" provision whereby an organization may: "collect, use or disclose personal information **only** in a manner and for purposes that a reasonable person would consider appropriate in the circumstances, whether or not consent is required under this Act."

- All relevant factors* must be take into account under subsection 12(2) in determining whether the manner and purposes are appropriate, including, if applicable:
  (a) the **sensitivity** of the personal information;
  (b) whether the purposes represent **legitimate business needs** of the organization;
  (c) the degree of **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.

- These sections codify principles set out in *Eastmond v. Canadian Pacific Railway*, 2004 FC 852 (CanLII), affirmed by the Federal Court of Appeal) in *Turner v. Telus Communications Inc* (2005 FC 1601), and have long been used by the OPC as elements of the test for determining the "reasonability" and appropriateness of the purposes of a given collection, use or disclosure.

**New inclusive requirement; former C-27 required consideration of an enumerated list of factors*

Purpose Identification and Data Minimization

- Organizations must **determine** and **record** the purposes associated with personal information that they collect, use or disclose **at or before the time of collection**, or before using or disclosing for a new purpose (s. 12(3) and (4))

- The "appropriate provisions" flow to the PPCDA's "limitation of collection" requirement, as organizations may only collect the personal information **that is necessary** for the determined and recorded purposes (s. 13)
  - The concept of "necessary" has been interpreted as akin to "required" and a higher standard than "mere reasonableness"
  - Operationalizing this principle within complex data ecosystems may prove very challenging

- If an organization contravenes the limitation of collection requirements at s. 13, the organization could be liable for an administrative monetary penalty of up to the greater of $10 million or 3% of gross global revenues (ss. 113-114)

De-Identification & Anonymization

"**Anonymize**" means to "irreversibly and permanently modify personal information to ensure that there is no reasonably foreseeable risk in the circumstances that an individual can be identified from the information, whether directly or indirectly, by any means" (s. 2(1))

"De-identify" means to "modify personal information so that an individual cannot be directly identified from it, although a risk of the individual being identified remains" (s. 2(1))

No Consent Needed to De-Identify or Anonymize:

- Organizations can use personal information to de-identify or anonymize it* without knowledge or consent (s. 20)

De-identified Personal Information is Personal Information:

- Personal information that has been de-identified remains personal information (s. 2(2))

De-identified Personal Information Carved Out of Data Subject Rights:

- Organizations are not required to fulfil the following rights requests in respect of de-identified personal information:
  - Disposal (s. 51(3))
  - Information and access (s. 63(2))
  - Amendment (s. 71(2))
  - Data mobility (s. 72(2))
- The obligation to maintain accuracy does not apply to de-identified personal information (s. 55(2))

**New; former C-27 contemplated authority for de-identification only*

De-Identification & Anonymization

De-Identification is a Condition Precedent to Relying on Certain Exceptions to Consent:

- Personal information must be de-identified in order to rely on the following exceptions to consent:
  - Use for an organization's internal research, analysis and development purposes (s. 21)
  - Use and disclosure for a prospective business transaction, unless the requirement to de-identify would undermine the objectives for carrying out the transaction (ss. 22(1) and (2))

Requirements for De-Identification Process:

- When de-identifying personal information, an organization must:
  - consider re-identification risk when applying technical and administrative measures to the information; and
  - ensure those measures are proportionate to the purpose for which the information is de-identified and its sensitivity (s. 74)

Prohibitions on Re-Identification:

- Organizations are **prohibited** from using de-identified personal information – alone or in combination with other information – to identify an individual, **except**:
  - to conduct testing of the **effectiveness of security safeguards** that the organization has put in place to protect the information;
  - where the personal information was de-identified **solely for the purpose of protecting the information**;
  - where one of the following **exceptions to consent in respect of the use** of personal information applies: ss. 18, 23, 24, 26, 27(2), 29(2), 30, 38(2) or 50;
  - where the personal information is used **solely for the purpose of anonymizing it**;
  - to **comply with any requirements** under the PPCDA or other federal or provincial law;
  - to conduct **testing of the fairness and accuracy** of models, processes and systems that were developed using de-identified personal information;
  - to conduct **testing of the effectiveness** of the de-identification process;
  - for a purpose or situation authorized by the Division under s. 138 (i.e., where, on an organization's request for authorization, the Division determines it is clearly **in the interests of the individual**); or
  - in any other **prescribed circumstance.** (s. 75)

- **Knowingly** using de-identified information in contravention of s. 75 is an offence, and an organization could be liable upon sentencing for a fine of up to the greater of $25 million and 5% of gross global revenues (s. 145)

Accountability Provisions

The PPCDA sets out provisions that clarify the concept of an "accountable organization" and several provisions relating to "demonstrable" accountability

- Background: Similar to PIPEDA, the PPCDA provides that organizations are "accountable" for personal information under their control

- The PPCDA clarifies that personal information is under the control of an organization (i.e., the accountable 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 (s. 7(2))

Accountability Provisions

- The PPCDA requires organizations to:
  - Designate one or more individuals as responsible for compliance with the Act (s. 7(2)
  - Implement and maintain a **privacy management program** that:
    - **includes policies, practices and procedures** that are put in place to fulfil the organization's obligations under the Act (s. 9(1)); and
    - **takes into account the volume and sensitivity** of personal information under the organization's control (s.9(2))
- Upon request (i.e., no reasonable grounds necessary), the Commission may require organizations to **provide access to the policies, practices and procedures** included in their privacy management program (s. 10(1))
- After reviewing these materials, the Commission may **provide guidance** on, or **recommend corrective measures** in relation to, the organization's privacy management program (s. 10(2))
- Organizations may also **voluntarily request guidance** from the Commission regarding their privacy management program (s. 76(c)(v))
- The Commissioner cannot use information obtained through the above mechanisms (s. 10 or 76(c)(v)) to initiate a complaint or carry out an audit, unless the Commissioner considers that the organization has **willfully disregarded** the corrective measures recommended in relation to its privacy management program (s. 87)

Service Providers – Concept Clarifications

Scope of Statutory Requirements

- Service providers must:
  - comply with statutory safeguarding requirements (s. 56); and
  - notify an accountable organization about a breach of security safeguards involving personal information under the organization's control as soon as feasible in the event of a security breach (s. 61)

- Service providers are expressly not subject to the PPCDA's provisions relating to accountability, consent, retention, accuracy, rights of access, transparency, data mobility and other Part 1 requirements in respect of personal information that is transferred to them under the control of the "accountable organization" (s. 11(2))

- However, a service provider that collects, uses or discloses personal information for any other purpose would effectively be deemed an "accountable organization" and would be subject to Part 1. (s. 11(2))

Service Providers and Consent

- The PPCDA clarifies that organizations may transfer an individual's personal information to a service provider without the consent of the individual to whom the personal information relates (s. 19)

Service Providers – Concept Clarifications

Service Providers and Disposal of Personal Information

- Where an accountable organization disposes of (i.e., permanently and irreversibly deletes or anonymizes) personal information at an individual's request, it must, as soon as feasible, inform any service provider to which it has transferred the information of the request and ensure that the service provider disposes of the information (s. 54(5))

Specific Enforcement Powers Impacting Service Providers

- Under s. 113(1), the Commissioner may issue a notice of contravention and impose a penalty for a contravention of the following service provider related provisions:
  - s. 56(1) – an organization (including a service provider) must protect personal information through physical, organizational and technological security safeguards
  - s. 11(1) – an organization that transfers personal information to a service provider must ensure that the service provider provides an equivalent level of protection to that which the organization is required to provide
  - s. 61 – a service provider must notify the accountable organization that any breach of security safeguards has occurred, as soon as feasible

- The maximum administrative penalty under this section 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 (s. 114)

Transfers/Disclosures Outside of Canada

PPCDA introduces a new federal requirement, prior to transferring or disclosing personal information outside of Canada, to:

(a) carry out a **privacy impact assessment** (in accordance with prescribed requirements); and

(b) **implement measures to mitigate risks** identified in the assessment (e.g., contractual safeguards, adherence to a code of practice or certification process approved by the Division or other prescribed measures)

A copy of an assessment must be provided to the Commission upon request

Accountability Frameworks – Codes of Practice and Certifications

The PPCDA provides statutory recognition of **codes of practice** and related **certification programs**

- Allows for the establishment of voluntary accountability frameworks that may be very helpful for personal information processing in complex data ecosystems, sectoral information sharing arrangements, AI and other complex analytics, business models, etc.
- Codes of practice must provide for "**substantially the same or greater protection of personal information as some or all of the protection provided**" under the Act (s. 92(2))
- **Criteria for codes and certification programs** to be set out in regulations (s. 142)
- Organizations **apply to the Division for approval** of a code or program (ss. 92(2) and 93(1)), and the Division makes public its decision regarding approval (s. 95)
- Compliance with a code or certification program does **not relieve an organization of its obligations under the Act** (s. 96)
- Certification programs run by entities will include **independent verification mechanisms** and **disciplinary measures** for non-compliance with the code (ss. 93(1)(d) and (e))

Accountability Frameworks – Codes of Practice and Certifications

The PPCDA provides statutory recognition of **codes of practice** and related **certification programs** *[cont'd]*

- The Commissioner's powers include (s. 85(2)):
  - requesting information from an entity operating an approved certification program (s. 85(2)(a));
  - cooperating with an entity operating an approved certification program (s. 85(2)(b));
  - recommending to the entity that an organization's certification be withdrawn in prescribed circumstances (s. 85(2)(c));
  - revoking the approval of a certification program, in prescribed circumstances as set out in regulations. (s. 85(2)(d))

- **Discretionary power to decline to investigate a complaint** (s. 98(1)): The Commissioner may decline to investigate where, among other grounds: (1) the complaint raises an issue covered by an approved certification program and the organization is certified under that program […] (5) the matter is already under investigation or has already been addressed via other procedures or under other federal or provincial law […] or (8) an investigation is unnecessary in the circumstances

- A penalty **cannot** be imposed if an organization was in compliance with an approved certification program at the time of the contravention. (s. 113(3)(a)), **BUT** the **private right of action** would still be available (s. 132) for the contravention

Protection of Children's Personal Information

- The **Commissioner**, the **Division** and **Commission** must consider the **best interests of children** in exercising powers or performing duties or functions under the PPCDA* (ss. 86(d), 90(d), 77(d))

- A child's personal information is contemplated within the definition of **sensitive** personal information (s. 2(1))
  - A "child" is an individual **under 18 years old*** (s. 2(1))

- Where children's personal information is sensitive, it **impacts other requirements**, including:
  - Privacy management programs (s. 9(2))
  - "Appropriate" purposes requirement (s. 12(2)(a))
  - Form of consent (s. 15(5))
  - Retention periods (s. 52(2))
  - Safeguarding obligations (s. 56(1))
  - Breach reporting and notification requirements (s. 58(8)(a))
  - Transparency obligations (s. 62(2)(e))
  - De-identification measures (s. 74(b))

**New requirement and definition not contained in former C-27*

Protection of Children's Personal Information

- **Rights and recourse** under the PPCDA may be exercised **on behalf of a child** by a parent, guardian or tutor, unless the **child wishes to personally exercise those rights** and is capable of doing so (s. 4(a))

- **Disposal requests** based on withdrawn consent or information no longer being necessary **cannot be refused** on the basis that disposal would have an undue adverse effect on the accuracy or integrity of information necessary to providing a product/service **if the information relates to a child** (s. 54(2)(d))

Authority to Process Personal Information – Consent

Under the PPCDA (and similar to PIPEDA), organizations may not collect, use or disclose personal information without a legal authority set out under the Act (s 15(1)). There are two classes of legal authorities for processing: (i) consent or (ii) an exception to consent.

Key new features of the PPCDA's consent authority for processing:

Primacy of Consent as Authority for Processing:

- Drafting suggests a **clear intention to re-enforce the primacy of consent** as the authority for processing of personal information (despite widespread acknowledgement of the increasing challenges faced by organizations obtaining valid consent in a dynamic, constantly evolving data environment)

Form of Consent:

- The PPCDA provides that **express consent is the default** form of consent
  - Specifically, when an organization relies on consent as an authority for processing, the organization **must generally obtain an express form of consent** (s. 15(5))

- An **implied form of consent** may only be relied upon if 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 (s. 15(4))
  - Prohibition on relying on implied consent if personal information is collected or used for prescribed "business activities" (ss. 15(6) and 18(2)) or collected, used or disclosed on the basis of having a legitimate interest (ss. 15(6) and 18(3))

Authority to Process Personal Information – Consent

Valid Consent

- The PPCDA provides **prescriptive information requirements** for obtaining a valid consent
- The information must be **provided** in **plain language** that an individual to whom the organization's activities are directed would reasonably be expected to understand at or before the time the individual seeks the consent (s. 15(4))
- The information must include the following content (which is more prescriptive than the meaning of "valid consent" under Section 6.1 of PIPEDA) (s. 15(3)):

  (a) the **purposes for the collection, use or disclosure** of the personal information determined by the organization and recorded under the Act's "appropriate purposes" provisions (in 12(3) or (4));

  (b) **the manner 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.

- An individual may, subject to limited exceptions, withdraw consent in whole or part to the collection, use or disclosure of their personal information (s. 17(1))

Exceptions to Consent – Standard Business Activities

The PPCDA clarifies and expands the circumstances where organizations may collect and/or use personal information without consent in the course of standard "business activities".

- No consent required for organizations to **transfer personal information to their third-party service providers** (s. 19)
- No consent required for the use of personal information to **de-identify or anonymize** it (s. 20)
- No consent required for the collection and use (**but not disclosure**) of personal information for "business activities" that: (18(1))
  - **i. are necessary to provide a product or service** that the **individual has requested** from the organization
  - ii. are necessary for **the organization's information, system or network security**;
  - iii. are necessary for the **safety of a product or service** that the organization provides or delivers;
  - iv. otherwise amount to a prescribed activity, (s. 18(2))

  provided that in the course of any activity:
  - the collection or use is something a **reasonable person would expect**; and
  - the collection or use **is not used to influence the individual's behaviour or decisions** (18(1))

Exceptions to Consent – Legitimate Interests

- Substantively distinct from GDPR "legitimate interests" authority
- Collection, use **or disclosure*** of personal information without consent is authorized if done for the **purpose of an activity in which the organization has a legitimate interest that outweighs any reasonably foreseeable adverse effect on the individual** that could result from that collection, use or disclosure, and:
  - **(a)** a reasonable person would expect the collection, use or disclosure for such an activity; and
  - **(b)** the personal information is not collected, used or disclosed for the purpose of influencing the individual's behaviour or decisions (s. 18(3))
- Before collecting, using or disclosing personal information in reliance on s. 18(3), an organization must**:**
  - **(a) identify and describing the organization's legitimate interest** in the proposed activity;
  - (b) carry out, in accordance with regulations, **a privacy impact assessment***, in which the organization must identify any **reasonably foreseeable adverse effect** on the individual that is likely to result;
  - Identify and take **reasonable measures to reduce likelihood of adverse effects** or to mitigate them; and (s. 18(4))
  - comply with any prescribed requirements (s. 18(4))
- **A record of such assessment** must be created and, upon request, provided to the Commission (s. 18(5))

**New: expansion of authority to disclose and explicit requirement to conduct a PIA, neither contained in former C-27*

Exceptions to Consent – Business Transactions

- Background: PIPEDA contains a helpful (and widely used) exception to consent for parties to disclose personal information in connection with a prospective and completed business transaction as long as certain requirements are met (including notice to impacted individuals upon completion of the transaction)

- The PPCDA contains a similar "**business transaction**" provision, but it has been amended very restrictively to require that personal information be **de-identified before it is used or disclosed** in connection with a prospective transaction (and remain de-identified until the transaction is complete)

- This de-identification requirement will not apply if:
  - de-identifying would "undermine objectives for carrying out the transaction", and
  - the organization has "taken into account the risk of harm" to the individual that could result from using or disclosing the information (s. 22(2))

Exceptions to Consent – Internal Research, Analysis and Development

- The PPCDA provides organizations with an exception to consent for the use of personal information for the broad concept of "internal research, analysis and development purposes", on the **condition** that the information be **"de-identified" prior to the use** for such purpose (s. 21)
  - Unlike exception to consent for business transactions, no carve-out where de-identification would "undermine the objective" of the R&D or analysis activity
  - Many R&D activities and analysis that legitimately require the processing of personal information (including standard customer research, AI and other complex analytics) would fall outside the scope of this exception to consent authority

- The PPCDA removes the disclosure exception for "statistics, study or research purposes" (former C-27, s. 35). There is no equivalent in Bill C-36.

Exceptions to Consent – Fraud Detection

- The PPCDA contains a "fraud exception" that **clarifies a technical drafting issue** under PIPEDA's exception to consent for fraud detection and suppression
  - PIPEDA provides an exception to the consent requirement for the **disclosure** of personal information to another organization where it is reasonable for the purposes of detecting or suppressing fraud or of preventing fraud. However, PIPEDA does **not** contain an express corresponding exception to the consent requirement for the **collection** of personal information for these purposes.

- The PPCDA clarifies that the exception to consent applies to **both** the **disclosure and corresponding collection and use** of personal information for the purposes of detecting, suppressing or preventing fraud (s. 27(2))

Exceptions to Consent – AML/TF

- The PPCDA includes the same consent exception as was recently added to PIPEDA via Bill C-69, which permits the **disclosure (and corresponding collection and use) of personal information without consent**, provided it is shared under s. 11.01(1) of the *Proceeds of Crime (Money Laundering) and Terrorist Financing Act* (PCMLTFA) (s. 41)

- Only entities referred to in s. 5 of the PCMLTFA may avail themselves of this exception, and only where the following four conditions are met:
  - the information was collected in the course of the entity's activities;
  - disclosure is reasonable for detecting or deterring ML/TF/sanctions evasion;
  - obtaining consent would compromise the ability to detect or deter ML/TF/sanctions evasion; and
  - disclosure is made in accordance with PCMLTFA regulations

- Entities under s. 5 of the PCMLTFA include banks, credit unions, trust and loan companies, life insurers, securities dealers, and money services businesses

Transparency and Openness

- The PPCDA requires organizations to make information that explains its policies and practices "**readily available**, in **plain language**" (s. 62(1))
  - PIPEDA requires organizations to be open about their policies and practices, and to make information available in a form that is "generally understandable"
- The PPCDA supplements PIPEDA's transparency requirements by setting out several new content requirements when organizations make such information available (s. 62(2)):
  - **How the organization applies consent exceptions** to its practices, including a description of any activities referred to in subsection 18(3) in which it has a **legitimate interest** (s. 62(2)(b))
  - A general account of **any automated decision systems** that could have **a legal or similarly significant effect** on individuals (see next slide) (s. 62(2)(c))
  - Whether or not the organization **transfers or discloses personal information internationally or interprovincially** that may have **reasonably foreseeable privacy implications** (s. 62(2)(d))
  - The **retention periods applicable to sensitive personal information** (s. 62(2)(e))
  - How individuals may make **a request for the disposal** (permanent and irreversible deletion or anonymization) of their personal information (s. 62(2)(f))
- Failure to comply may result in a penalty

Automated Decision Systems and Transparency

- "Automated decision system" is defined as "any technology that assists or **replaces the judgment of human decision-makers** through the use of a rules-based system, regression analysis, predictive analytics, machine learning, deep learning and a neural network or other technique" (s.2(1))
- New requirements apply to the use of automated decision systems to make **predictions, recommendations or decisions** about individuals that could have a **legal or similarly significant effect** on individuals
  - Openness: Organizations must make available a **general account** of the organization's use of any automated decision system (as noted in previous slide) (s. 62(2)(c))
  - Access: Upon request, organizations must provide individuals with a **plain language explanation** of any prediction, recommendation or decision made by an automated decision system (s. 63(4))
    - The explanation must indicate **the type of personal information** that was used to make the prediction, recommendation or decision, the **source of the information**, and the **reasons/principal factors** that led to the prediction, recommendation or decision (s. 63(5))
- Right to submit representations*: The organization must provide an individual with an opportunity to make **written representations** to an employee of the organization who is able **to review the prediction, recommendation or decision** that was made about them. (s. 63(6))
  - There is no express right to object to automated decisions
- Only contravention to the openness requirement may result in a penalty

**New right not contained in former C-27*

Breaches of Security Safeguards

- The PPCDA contains a similar mandatory breach notification requirement as under PIPEDA (s. 58)
- The PPCDA clarifies that **service providers** are required to notify the **organization that controls the personal information** of a breach of security safeguards (s. 61)
- The **form and content requirements** for the report to the Commissioner and notice to affected individuals will be prescribed by regulation
- **Penalties**: If an organization contravenes the breach notification requirements at s. 58, or the safeguarding requirements at s. 56(1), penalties may be imposed by the Commission and the organization could be liable for a fine of up to the higher of $10 million or 3% of gross global revenues (s. 113(1))
- **Fines**: If an organization **knowingly** contravenes the breach notification requirements at s. 58 or breach recording requirements at s. 60(1), the contravention may be prosecuted as an offence in court and the organization could be liable for a fine of up to the higher of $25 million or 5% of gross global revenues (s. 145)

New Right of Disposal of Personal Information

- **Upon request of an individual, an organization must dispose** of that individual's personal information if (subject to exceptions – see next slides):
  - The information was collected, used or disclosed in contravention of the Act;
  - The individual has withdrawn their consent, in whole or in part, to the collection, use or disclosure of the information; or
  - The information is no longer necessary for the continued provision of a product or service requested by the individual (s. 54 (1)((a)-(c))

- **Deepfakes**: The Government of Canada has framed the new right of disposal as a "right to request deletion," including to enable Canadians to ask that an organization "take down" deepfakes based on their likeness (Government of Canada, Technical Briefing on Bill C-36, June 17, 2026)

New Right of Disposal of Personal Information

- Key requirements/features of the right of disposal include:
  - Disposal means to "**permanently and irreversibly delete** personal information or to **anonymize** it" (s. 2(1))
  - Disposal must take place "**as soon as feasible**" after the request
  - Organizations must **inform any service provider** as soon as feasible about the request and ensure that the service provider disposes of the personal information (s. 54(5))

- Contravention of the retention and disposal requirements at ss. 52, 54(1) or 54(5) could expose an organization to a **penalty** of up to the higher of $10 million or 3% of gross global revenues (ss. 113-114)

Exceptions to the Right of Disposal of Personal Information

- Disposal requests based on withdrawn consent or information no longer being necessary **may be refused where:**
  - Disposal would result in the disposal of **personal information about another individual** and the information **cannot be severed** without imposing an undue burden on the organization*;
  - There are **legislative requirements** or **reasonable terms of a contract** that prevent it from doing so;
  - The information is necessary for the **establishment of a legal defence** or in the **exercise of other legal remedies;**
  - The information **does not relate to a child** and disposal would have an **undue adverse effect on the accuracy or integrity of information** necessary to the ongoing provision of a product/service to the individual in question;
  - The request is **vexatious or made in bad faith**; or
  - Disposal would have an **undue adverse effect on the organization** that outweighs any potential adverse effect on the individual resulting from the retention of the information – in this case, the organization must inform the Commission (s. 54(2)(a)-(f))

- Organizations are **not** required to dispose of **de-identified personal information** (s. 54(3))

**Undue burden qualification re: severability not contained in former C-27*

Data Mobility

The PPCDA includes a new* data mobility right:

- Upon request of an individual, an organization must disclose the personal information that it has collected from the individual to an organization designated by the individual (s. 72(1))
  - An organization is **not required** to disclose de-identified personal information (s. 72(2))
- The data mobility disclosure must take place "**as soon as feasible**" (s. 72(1))
- Both organizations must be subject to a "**data mobility framework**" provided under the **regulations** of the Act (s. 72(1))

**Note that data mobility was first introduced as an amendment to PIPEDA via Bill C-15 (Budget Implementation Act, 2025). Bill C-36 carries forward substantially the same provisions into the PPCDA (ss. 72 and 140).*

Data Mobility: Open Banking Context

- Open banking is the first federal use case operationalizing the data mobility provisions under PIPEDA/the PPCDA
- The federal government passed the *Consumer-Driven Banking Act* (CDBA) in 2024, which was materially reformed (prior to coming into force) by Bill C-15, the *Budget Implementation Act, 2025*
- The CDBA creates a framework to both enable consumers, including small businesses, to securely share prescribed types of financial data among defined participating entities, and to foster competition in the financial sector in the interests of consumers

Data Mobility Regulations

Key details about the **nature, scope and requirements of data mobility rights will be set out in regulations** (s. 140) that will contemplate:

- data mobility frameworks prescribing:
  - **safeguards** that must be put in place by organizations to enable the secure disclosure and secure collection of the personal information (s. 140(a)(i)); and
  - **parameters for the technical means for ensuring interoperability** in respect of the disclosure and collection of that information. (s. 140(a)(ii)),
- requirements **specifying organizations that are subject to a data mobility framework** (s. 140(b)); and
- requirements that provide for **exceptions to the data mobility disclosure requirement**, including exceptions related to the protection of proprietary or confidential commercial information (s. 140(c))

Osler's National Privacy and Data Management Practice


Adam Kardash


Éloïse Gratton

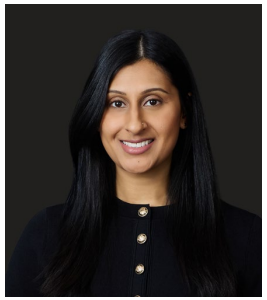

Joanna Fine


John Salloum


François Joli-Coeur


Adam LaRoche


Katelyn Smith

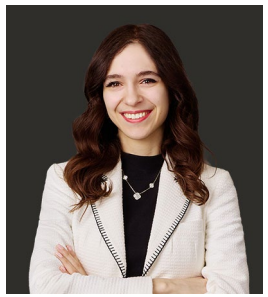

Komil Joshi


Tina Saban


Catherine Hart


Maryna Polataiko


Erika Romanow


Alannah Safnuk


Naomi Chernos


Marguerite Rolland


Alex Toma


Cassandre Legault


Colleen Morawetz

Thank you for attending!