WeirFoulds LLP

Bill C-36 and the Future of Canada's Federal Private Sector Privacy Law: What Has Changed, What It Means, and What to Do Now

June 19, 2026

By Olalekan (Wole) Akinremi and Thomas Harding, Summer Student

Introduction

Canada's federal private sector privacy reform has returned, and it is not merely Bill C-27 in revised form. On June 15, 2026, the federal government introduced Bill C-36, *An Act to enact the Protecting Privacy and Consumer Data Act, to amend the Personal Information Protection and Electronic Documents Act and to make amendments to other Acts*, marking the latest attempt to modernize Canada's private sector privacy framework following the failure of Bill C-27 to advance through Parliament before prorogation early last year.

Bill C-36 would enact the *Protecting Privacy and Consumer Data Act* ("**PPCDA**"), while Bill C-27 would have enacted the Consumer Privacy Protection Act ("**CPPA**"), a separate *Personal Information and Data Protection Tribunal Act*, and the *Artificial Intelligence and Data Act* ("**AIDA**"). The structural shift is significant: Bill C-27 was an omnibus package addressing privacy, tribunal oversight, and AI regulation in a single legislative instrument. Bill C-36, by contrast, is a focused privacy and consumer data bill.

Bill C-36, as currently drafted, reflects a more operationally focused approach, centering on privacy and consumer data while placing increased emphasis on accountability mechanisms, cross-border data governance, and risk-based standards.

If enacted in its current form, Bill C-36 would repeal Part 1 of the *Personal Information Protection and Electronic Documents Act* ("**PIPEDA**"). This would result in a fundamentally redesigned federal privacy regime.

What follows is an examination of the changes that, in our view, matter most.

Artificial Intelligence Unbundled: A Privacy-Focused Bill

For businesses, legal teams, and technology leaders, the first and perhaps most striking difference is that AI regulation has been effectively unbundled from the privacy bill. Bill C-27 included the proposed AIDA, a standalone statute within the omnibus bill that would have established a regulatory framework for high-impact AI systems, including requirements for risk assessments, bias mitigation measures, public reporting obligations, ministerial orders, and AI-specific offences.

Bill C-36 contains no equivalent AI legislation. It is framed squarely as a privacy and consumer data bill.

The PPCDA does retain the concept of "automated decision systems" and requires organizations to provide explanations to individuals where such systems are used to make predictions, recommendations, or decisions that could have "a legal or similarly significant

effect" on them. Organizations must also provide a general account of their use of automated decision systems in their publicly available privacy policies.

A Redesigned Regulatory Model

Bill C-27 relied on two bodies: the Privacy Commissioner of Canada for investigations and the proposed Personal Information and Data Protection Tribunal to hear appeals and impose administrative monetary penalties. Bill C-36 replaces this model entirely. It establishes the Digital Safety and Data Protection Commission of Canada (the "**Commission**"), a Privacy and Consumer Data Commissioner (the "**Commissioner**"), and a Privacy and Consumer Data Division (the "**Division**"). Critically, appeals under Bill C-36 are subject to review by the Federal Court rather than a specialized tribunal.

Under Bill C-36, the Commission would consist of five full-time members appointed by the Governor in Council. The Commissioner would lead investigations and compliance activities, while the Division would handle functions such as the approval of codes of practice and certification programs.

An entity may apply to the Division for approval of a code of practice that provides for substantially the same or greater protection of personal information as the PPCDA, and may also apply for approval of disciplinary measures for non-compliance with such a code, including the revocation of an organization's certification.

Practical Consequences of Proposed Regulatory Model

- This restructuring has notable practical consequences. The elimination of the proposed Personal Information and Data Protection Tribunal means that enforcement decisions will ultimately be subject to Federal Court review. While the Federal Court is a well-established forum, it operates under a different standard of review and procedural framework than a specialized privacy tribunal would have. For organizations, the shift also means that the Commission will play a more centralized role, combining investigative, advisory, and quasi-adjudicative functions within a single body.
- Legal departments should pay close attention to the procedural rules the Commission develops, as these will shape the practical landscape of privacy enforcement in Canada.
- It remains to be seen what impact the Commission and the Commissioner will have on the existing powers of the Privacy Commissioner of Canada. It will be worth watching for any statements issued by the Privacy Commissioner of Canada, Philip Dufresne, regarding the impact of Bill C-36 and its apparent encroachment on his office's powers.

Evolving Definitions and Clarified Terminology

Several definitional changes in Bill C-36 will have meaningful practical implications.

"Anonymize"

The most significant is the revised definition of "anonymize". Under Bill C-27, to anonymize meant "to irreversibly and permanently modify personal information, in accordance with generally accepted best practices, to ensure that no individual can be identified from the information, whether directly or indirectly, by any means." Under Bill C-36, the definition has shifted to a risk-based standard: to 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."

This is a substantial shift. Bill C-27 set an absolute standard: organizations had to ensure that "no individual can be identified." Bill C-36 adopts a contextual, risk-based approach, requiring organizations to ensure there is no "reasonably foreseeable risk" of

identification “in the circumstances.” This is consistent with the standard under Quebec’s *Regulation respecting the anonymization of personal information*. In practice, this means anonymization assessments will need to be tailored to the specific context, including factors such as the nature of the data, available re-identification techniques, and the environment in which the anonymized data will be used. Organizations should welcome the added flexibility, but should also be prepared to document their risk assessments thoroughly.

“Personal Information”

The definition of “personal information” has also been expanded under Bill C-36. It now includes information that is inferred about the individual. This is a notable expansion with significant implications for organizations that use data analytics, profiling, or AI systems to generate inferred data about individuals, as such inferred data would be treated as personal information and subject to the requirements under the PPCDA.

“Sensitive”

Bill C-36 also introduces a new defined term, “sensitive,” which “describes personal information in respect of which, taking into account the circumstances, an individual has a heightened expectation of privacy.”

The definition includes a non-exhaustive list of categories including:

- a child’s personal information;
- information revealing an individual’s racial or ethnic origin;
- political opinions;
- religious or philosophical beliefs; and
- biometric information capable of uniquely identifying an individual.

Under Bill C-27, the personal information of minors was simply “considered to be sensitive information” by statutory interpretation, without the broader definitional framework now provided.

The introduction of “sensitive” as a standalone defined term is more than a drafting refinement. It provides a clearer foundation for the several provisions throughout the PPCDA that impose heightened obligations in respect of sensitive personal information. In preparation for the PPCDA, organizations should review their data inventories and classification frameworks to ensure that information falling within this definition is treated appropriately.

Obligations Regarding De-Identification

Bill C-36 introduces more prescriptive requirements for de-identification. Under Bill C-27, organizations that de-identified personal information were required to ensure that technical and administrative measures were “proportionate to the purpose for which the information is de-identified and the sensitivity of the personal information.”

Bill C-36 adds a further obligation: organizations must also “consider, when applying technical and administrative measures to the information, the risk of an individual being identified.” This additional requirement reinforces the risk-based approach that runs throughout the bill and creates a stronger link between de-identification practices and the overall risk profile of the data.

Cross-Border Transfers and Required Privacy Impact Assessment

Cross-border transfers of personal information are subject to significantly more explicit requirements under Bill C-36 than under Bill C-27. Bill C-27 contained no specific cross-border transfer provisions of this nature within the CPPA itself.

Bill C-36 now requires that, before disclosing or transferring personal information outside Canada, an organization must carry out a privacy impact assessment in accordance with prescribed requirements and implement risk mitigation measures, such as contractual privacy protections, adherence to a code of practice, or a certification process approved by the Division. On request, an organization must also provide the Commission with access to, or a copy of, the privacy impact assessment.

These requirements have significant practical implications for vendor contracting, cloud computing arrangements, outsourcing relationships, and global data architecture. Organizations that routinely transfer personal information outside Canada, whether to affiliates, service providers, or cloud infrastructure located abroad, will need to build privacy impact assessments into their transfer workflows.

Breach Reporting – An Area of Continuity

One area of continuity between the two bills is breach reporting. Both Bill C-27 and Bill C-36 require an organization to report to the applicable oversight body any breach of security safeguards involving personal information under its control, where it is "reasonable in the circumstances to believe that the breach creates a real risk of significant harm to an individual." While the reporting obligation itself remains substantively unchanged, the identity of the recipient has shifted: under Bill C-27, reports would have been made to the Privacy Commissioner of Canada, whereas under Bill C-36, they are directed to the Commission.

"Legitimate Interest" – Collecting, Using, and Disclosing Personal Information Without Consent

The legitimate interests exception has been expanded and refined under Bill C-36, making it both more commercially useful and more tightly regulated.

Under Bill C-27, an organization could collect or use personal information without consent where a legitimate interest outweighed the potential adverse effects on the individual. Bill C-36 extends this exception to collection, use, or disclosure, broadening the scope of activities that can be undertaken without consent under this ground.

However, Bill C-36 also imposes stricter conditions. Before relying on the legitimate interests exception, an organization must;

- identify and describe its legitimate interest in the proposed activity;
- carry out a privacy impact assessment identifying any reasonably foreseeable adverse effects on the individual;
- identify and take reasonable measures to reduce, mitigate, or eliminate those effects; and
- comply with any prescribed requirements.

The organization must also record its description of the legitimate interest and, on request, provide the Commission with access to both the description and the assessment.

For organizations, the practical takeaway is twofold. The extension of the legitimate interests exception to disclosure activities creates new flexibility, particularly for data sharing arrangements. At the same time, the requirement to conduct and record a privacy impact assessment, and to produce it to the Commission on request, means that organizations relying on this exception must be able to demonstrate, with documented evidence, that their use of personal information is proportionate and justified. This is a meaningful step beyond what Bill C-27 would have required.

Remedies

Administrative Monetary Penalties

The administrative monetary penalty framework under Bill C-36 remains largely consistent with Bill C-27. The maximum penalty for all contraventions found in a single investigation is the greater of $10,000,000 and 3% of the offending organization's gross global revenue in its financial year before the one in which the penalty is imposed.

However, there is one important structural difference. Under Bill C-27, administrative monetary penalties were recommended by the Privacy Commissioner of Canada and imposed by the Personal Information and Data Protection Tribunal. Under Bill C-36, the Commissioner can include a penalty in a notice of contravention, and the Commission reviews the matter if the organization applies for a review. This consolidation of the penalty process within the Commission framework streamlines enforcement but also concentrates significant power in a single body.

Offences

For knowing contraventions of certain provisions, both bills provide for offences with fines of up to $25,000,000 or 5% of gross global revenue on indictment, and up to $20,000,000 or 4% of gross global revenue on summary conviction. These thresholds remain unchanged between the two bills.

Organizations should note that the factors the Commission must consider in determining penalty amounts include:

- the nature and scope of the contravention;
- evidence of due diligence;
- reasonable mitigation efforts;
- compliance history;
- the organization's ability to pay; and
- any financial benefit obtained from the contravention.

Private Right of Action

Both Bill C-27 and Bill C-36 provide a private right of action for individuals affected by an organization's contravention. Under both bills, an individual has a cause of action for damages for loss or injury suffered as a result of a contravention, subject to certain conditions.

Under Bill C-27, the right of action could be exercised following a finding by the Commissioner that was either not appealed or was upheld by the Tribunal. Under Bill C-36, the right of action is available following a finding by the Commissioner under the new enforcement framework, subject to the applicable review and appeal processes, including review by the Commission and appeal to the Federal Court.

For organizations, the private right of action remains a significant source of potential liability.

Conclusion and Next Steps

Bill C-36 represents a deliberate recalibration of the federal government's approach to privacy reform. By removing the standalone AI regulatory framework and concentrating its efforts on a focused, operationally grounded privacy bill, the federal government has signalled that the immediate priority is modernizing Canada's core private sector privacy regime. The result is a bill that, while sharing

much of the foundational structure of Bill C-27, introduces meaningful refinements in key areas.

Organizations that will be best positioned under the new regime will be those that take proactive steps now. This includes:

- reviewing data governance frameworks;
- updating privacy impact assessment processes;
- assessing cross-border data flows; and
- ensuring that internal policies and practices can withstand the level of documentation and accountability that Bill C-36 demands.

As this bill progresses through Parliament, further amendments are possible. We will be monitoring developments closely and providing updates as events unfold.

If you have any questions, please contact the Privacy & Access to Information team.

The information and comments herein are for the general information of the reader and are not intended as advice or opinion to be relied upon in relation to any particular circumstances. For particular application of the law to specific situations, the reader should seek professional advice.

For more information or inquiries:

Olalekan (Wole) Akinremi

Toronto
416.947.5049

Email:
oakinremi@weirfoulds.com

Olalekan (Wole) Akinremi is a Partner in the Technology & Intellectual Property and Privacy & Access to Information Practice Groups at WeirFoulds LLP.