David Young Law
Compliance Bulletin

July 2026

Privacy Bill – The key provisions (1)

On June 15, the federal government tabled its long-awaited, updated privacy reform law, Bill C-36, the *Protecting Privacy and Consumer Data Act* (PPCDA). The Bill should be seen as the second in the government's one-two punch of putting specifics on the generalities of its national AI Strategy, "AI for All", announced June 4.[1] The Bill is closely linked to Bill C-34,[2] the proposed new online harms legislation - reflecting the government's coordinated approach to not only updating the privacy law to respond to current digital realities, but also to addressing harms arising out of the misuse of personal information, with particular focus on the online medium. Together, these proposed laws will enable the government to show that it is concerned with the safety of Canadians in the new digital (read AI-driven) world as it is promoting innovation and the growth potential offered by that world.

This *Bulletin* reviews the broad oversight and enforcement framework proposed by Bill C-36. A second *Bulletin* will review the key compliance rules provided under the Bill.

It will be remembered that in its last attempt at enacting a reformed privacy law – Bill C-27 – the government included a broad-scope AI governance law, the *Artificial Intelligence and Data Act*, or "AIDA", with the goal of laying down an oversight framework to regulate high-risk AI. There was significant pushback to the proposed AI law, ranging from the criticism that there had not been sufficient consultation regarding its scope to the concern that any AI regulation at this time was premature and would stifle innovation.

In its AI Strategy the government articulated as one of its goals, to build trust in AI – in the words of the Prime Minister, to protect Canadians from the risks and harms of AI by modernizing legislative frameworks for the digital age that prioritize trust and safety and reduce the risks of AI.[3] In the apparent absence of an overall AI governance law as part of the Strategy, we must look to the reformed privacy law, as well as the online harms law, for precepts of transparency, risk assessment and risk mitigation that can address this goal.

Third time lucky?

While today, in 2026, we can parse through the now refined and updated provisions of the proposed PPCDA, it should be recalled that this is the government's third attempt at reform of the now 25-year-old privacy law, PIPEDA[4], going back to November 2020. What we have now is quite a lot like that original bill, Bill C-11, enacting the *Consumer Privacy Protection Act* (CPPA), but which in many detail points contains adjustments reflecting the consultations, stakeholder

[1] *Canada's National Artificial Intelligence Strategy: AI for All,* Innovation, Science and Economic Development Canada (ISED), June 8, 2026.
[2] *Safe Social Media Act,* First Reading, June 10, 2026.
[3] *Prime Minister Carney launches AI for All: Canada's new national artificial intelligence strategy,* June 4, 2026
[4] *Personal Information Protection and Electronic Documents Act*, S.C. 2000, c.5.

commentaries, and submissions to the parliamentary Industry and Technology Committee regarding both Bills C-11 and C-27.

The PPCDA maintains the "generally accepted privacy principles" of PIPEDA but moves the overall protective framework closer to the EU's *General Data Protection Regulation* (GDPR) – which came into force in 2018 and at that time seen as the cutting edge of "second generation" privacy laws. Furthermore, the PPCDA tracks closely the substantive privacy rules under its predecessor, the previously proposed CPPA, with a few, important, additions.

Analysis of Bill C-36 addresses a number of precepts as "new" in the context of the current privacy regulatory environment, as that has evolved under PIPEDA. However, one can argue that these are not really "new" since privacy stakeholders have become familiar with many of them through the legislative trajectories of Bills C-11 and C-27, and that these principles have been adopted as legislative rules both in Europe with the GDPR as well as in Quebec with Law 25 and in many US states – reflecting in lights the "past its due date" status of PIPEDA.

New enforcement framework

Bill C-36 tracks closely its predecessor, Bill C-27, with one main exception – the oversight and enforcement framework. While Bill C-27 included significant new powers for the Privacy Commissioner, including the ability to make compliance orders and seek significant financial penalties, appeals from the Commissioner's orders and imposing penalties were the purview of a separate body, the proposed Personal Information and Data Protection Tribunal. This body was to have a quasi-judicial role broadly comparable to the Competition Tribunal.

Bill C-36, together with Bill C-34, changes course completely. Firstly, and significantly, the Office of the Privacy Commissioner's (OPC) role for oversight of private sector privacy law is transferred to a new body, the *Digital Safety and Data Protection Commission of Canada*. The OPC's role will, henceforth, be limited to the oversight of public sector privacy, as regulated by the federal *Privacy Act*.

Secondly, the Commission will not only have responsibility for private sector privacy compliance, but also the primary oversight role for enforcing the *Digital Safety Act,* to be enacted as part of Bill C-34. The *Digital Safety Act* is a more articulated version of the government's previous attempt at passing online harms legislation (Bill C-63) minus the hate speech provisions but now including provisions regarding chatbots and a social media ban for children.

Within the new Commission a *Privacy and Consumer Data Division* will be established to focus on privacy compliance. It will be comprised of a Privacy and Consumer Data Commissioner and one other member of the Commission. The Division, presumably headed up by the new Commissioner, will have direct responsibility for oversight of the PPCDA. In particular, the Commissioner will have responsibility for investigating breaches and proposing remedies, including compliance orders and financial penalties.

Under the new oversight framework, it is clear that the actions of the Commissioner will be more closely aligned with the government's priorities which presumably, while ensuring privacy protection, may include advancing its innovation agenda. Firstly, by contrast with the current Privacy Commissioner who is an independent officer of Parliament, the new Commissioner will be appointed by the Governor in Council (i.e. Cabinet), with no role by Parliament. Secondly, there

will be a more active role for the government – more specifically the Minister responsible – in the Commission's development of guidance materials respecting the Commission's and the Division's exercise of powers in relation to enforcement and dispute resolution, as well as in connection developing regulations setting out criteria for approval procedures of codes of practice and certification programs.

While operating within the confines of the 25-year-old PIPEDA, the OPC has achieved some significant successes in responding to the challenges of today's privacy threats and in this regard, has worked closely with other Canadian as well as global privacy regulators.[5] It should be logical to suggest that the learned experience as well as the operational infrastructure developed within the OPC over the past 25 years will be retained and transferred to the Commission.

Codes of Practice and Certification Programs

As under Bill C-27, the Bill provides for adoption and approval of codes of practice and programs for certification under such codes as compliance standards for organizations that operate in a particular area involving data processing. Compliance with a code under a certification program will enable an organization to have confidence that its data processing policies and procedures meet the regulator's expectations for compliance and that the organization will not be subject to investigation or penalties.

The codes of practice and certification framework may be useful to organizations that operate complex data processing systems, participate in subject area data sharing relationships, utilize AI and other data analytics models, or otherwise engage in data processing activities that may involve particularized protocols not readily falling within the basic rules laid out by the privacy law. Alternatively, such a code could set out more articulated standards for compliance in a specific area, such as children's privacy, than are specified under the general statutory rules.

Bill C-36 stipulates that an entity (meaning not just an organization but also industry bodies such as standards-setting associations) may, in accordance with the regulations, apply to the Division for approval of a certification program. The program must include: a code of practice providing for substantially the same or greater protection of personal information as provided under the law; guidelines for interpreting and implementing the code; a mechanism for certifying that an organization is in compliance with the code; a mechanism for the independent verification of an organization's compliance with the code; and disciplinary measures for non-compliance, including revocation of an organization's certification.

To be noted, compliance with the requirements of a code of practice or a certification program does not relieve an organization of its obligations under the Act. However, a penalty cannot be imposed if an organization was in compliance with an approved certification program even if it was in contravention of a provision of the law, although the private right of action (see below) would still be available.

[5] See, for example, *Joint investigation of TikTok Pte. Ltd. by the Office of the Privacy Commissioner of Canada, the Commission d'accès à l'information du Québec, the Office of the Information and Privacy Commissioner for British Columbia, and the Office of the Information and Privacy Commissioner of Alberta*, PIPEDA Findings # 2025-003, September 23, 2025.

Remedies

Remedies under Bill C-36 will be proposed in a *Notice of Contravention* served on an organization which either may accept them or request their review by the Commission. If a remedy is not accepted by either the organization or a complainant (if applicable), the Commission will make a determination to confirm, cancel or vary the proposed remedy. If the organization does not pay a proposed financial penalty or request a review by the Commission, it will be deemed to have breached the provisions at issue and liable to pay the penalty.[6]

The remedies for non-compliance are substantially the same as provided under Bill C-27 – mandatory compliance orders, administrative monetary penalties of up to the greater of $10,000,000 or 3% of an organization's worldwide annual gross revenue, and fines for offences of up to $25,000,000 or 5% of an organization's worldwide gross revenue, whichever is greater.

As an alternative to a compliance order, the Commissioner and an organization may enter into a compliance agreement containing any terms that the Commissioner considers necessary to ensure compliance. Not specifically addressed in the Bill is the inclusion in any compliance agreement for payment of a financial penalty. However there is recognition that such an agreement may include damages for breach and, it can be surmised, can encompass scope for a financial payment in effect as an agreed penalty.

The Division also may attempt to resolve a matter by means of a dispute resolution mechanism such as mediation and conciliation, unless the matter is the subject of an application for review by the Commission.

Private right of action

As under Bill C-27, any individual who has been affected by an organization's contravention of the PPCDA may bring an action against the organization for damages for loss or injury suffered as a result of the contravention if: the Commissioner has made a finding of contravention which is not the subject of review or appeal, or the Commission has confirmed or varied the finding and the finding has not been appealed to the Federal Court or an appeal has been dismissed by the Court; if the Federal Court has made a finding of contravention; or if the organization has entered into a compliance agreement that does not provide for payment of damages.

A right of action also is available to an individual for damages resulting from an offence for which an organization has been convicted under the law.

For more information please contact: David Young 416-968-6286 david@davidyounglaw.ca

[6] The PPCDA's proposed framework for financial penalties and compliance orders is broadly analogous to that provided under the federal anti-spam law, CASL. Under that law, an offending organization that is served with a Notice of Violation stipulating a financial penalty is deemed to have committed the violation if the penalty is not paid or is not varied by the CRTC after application for review by the organization. The CRTC also may make compliance orders in relation to a violation.