David Young Law
Compliance Bulletin

July 2026

Privacy Bill – The key provisions (2)

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 is closely linked to Bill C-34,[1] 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.

This *Bulletin* is the second of two commentaries addressing the key provisions of the Bill. The first instalment reviewed the proposed new enforcement framework, in particular the transfer of private sector privacy oversight from the Office of the Privacy Commissioner (OPC) to the proposed *Digital Safety and Data Protection Commission of Canada*.[2] This *Bulletin* reviews key compliance rules under the Bill.

The PPCDA maintains the "generally accepted privacy principles" of the current law, PIPEDA,[3] 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 was 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 *Consumer Privacy Protection Act* (CPPA), with a few, important, additions.[4]

Privacy as a fundamental right

A key change from its predecessor, Bill C-27, is the recognition of privacy as a "fundamental right" – in the Purpose clause, section 5. The Purpose clause reflects one of the instances of the "balancing" rule as originally stated in PIPEDA and now found in the PPCDA – that individuals' rights to privacy must be considered in the context of the needs of organizations to collect and use their personal information, for purposes that a reasonable person would consider appropriate.

Missing from both Bill C-11 and Bill C-27 as originally tabled, privacy advocates had argued strongly for the recognition of privacy as fundamental human right, with constitutional status. Such recognition it was argued would provide the strongest level of protection of personal information in the context of ever-increasing encroachments for technology and commercial uses. The "fundamental" characterization of the privacy right in section 5 does not achieve this level of status. However, it can be argued that the addition of the descriptor "fundamental" strengthens the inherent nature of

[1] *Safe Social Media Act,* First Reading, June 10, 2026.
[2] See: Privacy Bill – The key provisions (1), DYL Compliance Bulletin July 2026.
[3] *Personal Information Protection and Electronic Documents Act.*
[4] As proposed under Bill C-11, the *Digital Charter Implementation Act, 2020* and Bill C-27, the *Digital Charter Implementation Act, 2022.*

the privacy rights protected under the Bill, particularly vis-à-vis the "balancing" provisions, as found in section 5, in the "appropriate purposes" provision in section 12, and in the "legitimate interests" rule in s. 18(3) (see below).

Appropriate purposes

In s. 12(1), Bill C-36 maintains substantially a key PIPEDA rule – that any collection, use or disclosure of personal information must meet the threshold of being for purposes that a reasonable person would consider appropriate in the circumstances, whether or not consent is required.

The rule has formed the basis of several important findings by the OPC regarding non-compliant collection and use of personal information in the digital environment, including TikTok's collection children's data for unauthorized targeting purposes[5] and ChatGPT's scraping the internet for information to populate its LLM databases.[6] Bill C-27 had proposed in effect limiting the factors to be considered as appropriate, which privacy advocates had argued would weaken the potential application of the rule.

Protections for children

Bill C-36 enhances the protection of children's information vis-à-vis Bill C-27, in several respects. The most significant change is the requirement that in connection with any investigation or decision under the PPCDA the oversight authorities must take into account as a factor "the best interests of the child".[7] The best interests of the child is a principle articulated in the evolving children's privacy laws in Europe and the US – as for example set forth in the UK's *Age appropriate design code for online services*. This requirement does not rise to the level of a principle as argued for by many children's advocates but should have the effect of ensuring that in circumstances involving the collection and use of children's information the highest level of protection will be considered, not only against misuse of such information but also against risks of harm.

Other provisions of the Bill strengthening privacy protections for children include stipulating that such information is considered sensitive and that as such requires the express consent of a parent for any collection, use or disclosure, both of which were substantially stipulated in Bill C-27.

However, the most impactful potential protections for children in the digital environment likely will be exercised by the new Commission through its authority to enforce the updated online harms law, the *Digital Safety Act*, as to be enacted by Bill C-34. That law if adopted will require platforms to conduct risk assessments for any online communications potentially interacting with children and to mitigate or eliminate such risks, or if that is not possible, to cease such communications.

[5] *Joint investigation of TikTok* , PIPEDA Findings # 2025-003, September 23, 2025.
[6] *Joint Investigation of OpenAI,* PIPEDA Findings #2026-002, May 6, 2026.
[7] As had been proposed by the Minister, at Committee, to be included in the preamble to Bill C-27.

A significant feature of that law is the potential for adoption of a statutorily-mandated design code for children, similar to that adopted in the UK and as proposed in several US states.[8]

De-identification and anonymization

Bill C-36 now provides for a complete framework for de-identification and anonymization of personal information, consistent with Quebec's Law 25 and with the criteria articulated by the Ontario Information and Privacy Commissioner (IPC).[9]

De-identify is defined to mean modifying personal information so that an individual cannot be directly identified from it, recognizing that a risk of re-identification remains. De-identified information continues to be personal information with the proviso that specific provisions of the law do not apply to it. In applying technical and administrative measures to de-identify information, an organization must consider the risk of an individual being identified and must ensure that those measures are proportionate to the purpose for de-identification as well as the sensitivity of the information.[10]

Anonymize is defined as irreversibly and permanently modifying personal information to ensure that there is no reasonably foreseeable risk that an individual can be re-identified, directly or indirectly by any means. The definition is a change from that in Bill C-27 which in effect provided for an absolute requirement that no individual could be identified from the information – generally considered to be an unattainable rule.

The standard of no reasonably foreseeable risk of re-identification is understood to be the appropriate criterion for anonymizing personal information for purposes of use outside the strictures of the privacy law. While the Bill does not contain the specifics of what that standard is – which are generally understood to be as articulated in cases and regulator guidance - it provides for those (optionally) to be set out in a regulation, which is the approach stipulated under the Quebec law.[11]

It may be expected that the government will adopt such a regulation, providing clear rules for meeting the standard and aligned with the Quebec criteria, thus enabling a uniform, readily referable reference for organizations seeking to make use of anonymized personal information for purposes not requiring identifiable information, such as research, surveys, testing of artificial intelligence (AI) models and more broadly, innovation.[12]

In s. 6(5), for clarity, it is stipulated that the PPCDA does not apply to anonymized information. However, it should be understood that the legislation will continue to apply with respect to the methodology and process used to anonymize personal information and, therefore, in effect, to the resulting anonymized information, in respect of any deficiencies vis-à-vis the requirements of the law.[13]

---

[8] See for example, *The California Age-Appropriate Design Code Act*.
[9] *De-identification Guidelines for Structured Data,* IPC, October 15, 2025.
[10] PPCDA, s. 74.
[11] See Quebec *Regulation respecting the anonymization of personal information, O.C. 783-2024* – considered to lay down generally accepted rules for meeting the standard, as well as acknowledging that eliminating all risk of re-identification is not required.
[12] As proposed by the government, in the 2025 Industry and Technology Committee hearings, but not accepted.
[13] In particular, compliance with respect to any downstream uses of the anonymized information.

Bill C-36 also adds a clarifying provision relative to Bills C-11 and C-27 – that no consent is required for an organization to either de-identify or anonymize personal information. Those previous versions provided an exception only for de-identification, which then left open the argument as to whether the exception extended to anonymization (to the effect that it would have been included as form of anonymization), without it being expressly being stated.

Valid consent

Bill C-36 stipulates explicit, enhanced requirements for valid consent – that it must be express – but recognizing that it may be implied in circumstances reflecting the reasonable expectations of the individual and is not sensitive. Furthermore, certain details must be provided by an organization requesting consent, in plain language so that they can be reasonably understood. The information to be provided includes the type of information involved and the purposes and the reasonably foreseeable consequences of its collection, use or disclosure. These explicit consent requirements go beyond what is set out currently in PIPEDA but are consistent with guidance provided by the OPC. They are broadly aligned with Quebec Law 25's enhanced requirements for consent.

However, the Bill fails to include PIPEDA's broader stipulation for valid consent – that an individual from whom consent is sought understands the nature, purpose and consequences of the collection, use or disclosure[14] - an omission that the current Privacy Commissioner as well as privacy advocates have argued is a deficiency in the proposed new law. This rule has been characterized as requiring "meaningful consent" which, it is argued, is a more strict rule than simply satisfying the information disclosure requirements for valid consent under Bill C-36. The s. 6.1 rule has been applied in several recent OPC investigations involving online data collection to find that meaningful consent was not obtained.[15]

Exceptions to consent – the legitimate interest exemption

A significant provision added in the Bill C-27 version of the proposed privacy reform law is the exception to consent for collection, use or disclosure of personal information for purposes of activities considered to be for an organization's "legitimate interest". This provision is similar to an analogous exception under the GDPR.

Essentially, it enables an organization to collect, use or disclose personal information without consent for purposes that an individual would reasonably expect provided that the organization's interest outweighs any reasonably foreseeable adverse effect on the individual that could result from that collection, use or disclosure. A key corollary condition is that the organization must have conducted a privacy impact assessment (PIA) with respect to the proposed activity and based on that assessment have taken steps to mitigate or eliminate any adverse effects identified.

The exemption is arguably analogous to an implied consent rule but without any requirement for consent - meaning that it is available for activities that an individual knows about and for which they expect the collection, use or disclosure of

[14] PIPEDA s. 6.1

[15] See, for example, ***Joint investigation of TikTok***, PIPEDA Findings # 2025-003, September 23, 2025.

their information. To be noted, an individual always the ability to request deletion of their personal information if no longer required for the supply of a product or service.[16]

The exemption can be seen as facilitating the use of personal information in the digital world, in particular online, where it is recognized that in many instances obtaining meaningful consent is impractical, unrealistic or effectively impossible. It also can be understood as a facilitator for use of personal information in AI applications and for supporting innovation more generally.

An important limitation however is that information collected and used pursuant to the exemption may not be used for purposes of influencing an individual's behaviour or decisions. In other words, it cannot be used for profiling purposes related to targeting the individual with communications and marketing pitches designed to influence their behaviour or decisions (such as purchase decisions).

Privacy Management Programs

Bill C-36 makes mandatory what has been the OPC's explicit guidance under PIPEDA – the requirement for organizations to establish and implement privacy management programs in order to ensure compliance with their obligations under the law.[17] Such programs must include policies, practices and procedures respecting: the protection of personal information; how requests for information and complaints are dealt with; the training and information provided to staff respecting the organization's policies, practices and procedures; and the development of materials to explain the those policies and procedures.[18]

In developing its privacy management program, the organization must take into account the volume of personal information that it is responsible for as well as the sensitivity of that information – meaning that the depth and details of an organization's program can (and should) be commensurate with the information that it holds.

To be noted, an organization must, on request, provide the Commission with a record of the documents constituting its program – i.e. its policies, practices and procedures. The Commission may, after reviewing the relevant documents, provide guidance or recommendations regarding any required corrective measures in relation to the program.

Algorithmic transparency

Related to the government's AI Strategy, which requires that AI use must be responsible and ethical, the Bill includes AI transparency provisions, as in Bills C-11 and C-27. These provisions require an organization to make publicly available in its policies a general account of its uses of automated decision systems (ADS) to make predictions, recommendations or

[16] Pursuant to the right to deletion, PPCDA, s. 54. This right also applies if the individual has withdrawn consent; it is not clear whether the right to deletion would apply in circumstances where the information is collected under s. 18(3) i.e. without consent, for purposes other than the supply of a product or service, such as for AI training purposes.
[17] See: *Getting Accountability Right with a Privacy Management Program*, Office of the Privacy Commissioner of Canada, Office of the Information and Privacy Commissioner of Alberta. Office of the Information and Privacy Commissioner for British Columbia; April 2012.
[18] PPCDA, s. 9.

decisions about individuals.[19] If the organization has used an ADS for such purposes that could have a legal or similarly significant effect on an individual, the organization is required to, on request, provide them with an explanation of that action including the type of personal information that was used, the source of the information and the reasons or principal factors that led to the prediction, recommendation or decision. Bill C-36 adds to these requirements the right of individuals to make representations – in other words, request a review - respecting the organization's action resulting from its use of personal information for these purposes.[20]

In sum, as now provided, the Bill stipulates algorithmic (read AI) transparency provisions that are broadly consistent with those stipulated under Quebec's Law 25 and under the GDPR.

Service providers and cross-border transfers

Bill C-36 provides a comprehensive framework for organizations in dealing with their service providers, in contrast to the cryptic rules provided under PIPEDA. [21] The Bill clarifies that transfers of personal information to service providers (i.e. for processing) may be made without consent and that the transferring organization, not the service provider, is responsible for compliance with the PPCDA's general rules in regard to that information. However, a service provider is responsible for complying with the statute's security requirements and for notifying the transferring organization in the event of a breach. As under PIPEDA, the transferring organization must ensure that the service provider provides an equivalent level of protection to that which the organization is required to provide.

A significant new rule that will impact many service provider relationships is the requirement for organizations transferring, or disclosing, personal information outside of Canada.[22] This rule requires an organization to conduct a PIA with respect to the transfer or disclosure in accordance with requirements stipulated by regulation, and to take measures to mitigate risks identified in that assessment. The proposed rule is aligned with the similar rule under Quebec's Law 25 and can be viewed as having its origins in the GDPR's transborder transfer rule. In its essence, the rule is directed at ensuring that personal information collected from Canadians, if transferred outside of Canada, will continue to have protection equivalent to that which it benefits from under Canadian law.

The transborder requirements to minimize risk, including the PIA requirement, should be understood as forming part of an organization's standard due diligence process for validating a cross-border service provider to which it is transferring data for processing. To be noted, the Bill C-36 rule specifically references contractual measures, which would be included in a service provider contract, typically as a matter of course. It can be further understood that the PIA and risk mitigation requirement should apply to transfers generally to a particular service provider which, once validated with appropriate contractual provisions, would continue in place with only a need to update these should circumstances change. Presumably, this format will be clarified by the anticipated regulations setting out requirements for PIAs.

[19] PPCDA, s. 62(2)(c).
[20] PPCDA s. 63(4)-(6).
[21] PPCDA, ss. 11, 19, 61.
[22] PPCDA s. 57

For transborder disclosures more generally (i.e. not to service providers), the PIA requirement may be addressed in part by the qualification of the offshore jurisdiction as meeting an "adequacy" criterion along the lines of the GDPR rule. Again, clarity and direction in this regard likely will be provided by the anticipated regulations.

Also to be noted is the requirement for organizations to include in their published privacy policies whether or not they transfer or disclose information internationally or interprovincially that may have reasonably foreseeable privacy implications.[23] This requirement also tracks similar provisions in Law 25 and the GDPR.

Right to deletion

As under Bill C-27, Bill C-36 provides for an express right of an individual to request an organization to delete their information, if they have withdrawn their consent, in whole or in part, to its collection, use or disclosure, or if the information is no longer required for the continued provision of a product or service requested by the individual. The right also applies if the information was obtained or processed by the organization in contravention of the law.[24]

This right has been framed by the government as extending to a takedown right respecting information posted on platforms online, including "deepfake" images.

The deletion obligation extends to informing an organization's service providers to which it has transferred the information of the request and ensuring that the service providers have deleted the information.

An organization is not required to delete personal information that has been de-identified.[25]

Data mobility right

Also as under Bill C-27, the Bill provides for the establishment of a data mobility framework, to be articulated by regulations.[26] It is anticipated that that first such framework will be developed for purposes of the financial services industry.

The right of an individual to mobility of their data mobility is understood to be an important element of their privacy rights – the right to transfer their personal information from one organization to another.

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

[23] PPCDA, s. 62(2)(d).
[24] PPCDA, s. 54 (Disposal at individual's request).
[25] PPCDA, s. 54(3).
[26] PPCDA, ss.72, 140. Also proposed as an amendment to PIPEDA pursuant to Bill C-15 *(Budget Implementation Act, 2025).*