Canada's new federal privacy Bill C-27 – Summary of significant impacts and new proposals

June 20, 2022

Authored by Kirsten Thompson, National Lead, Privacy and Cybersecurity

On June 16, 2022, the Canadian government tabled Bill C-27 "*An Act to enact the Consumer Privacy Protection Act, the Personal Information and Data Protection Tribunal Act and the Artificial Intelligence and Data Act and to make consequential and related amendments to other Acts.*"

The Bill is designed to update Canada's federal private sector privacy law, the *Personal Information Protection and Electronic Documents Act* (**PIPEDA**), to create a new tribunal, and to propose new rules for artificial intelligence (AI) systems.

Bill C-27 is a re-working of Bill C-11, *the Digital Charter Implementation Act,* that was introduced in November 2020, but died on the order paper with the announcement of the federal election. Notably, a significant portion of Bill C-11 has been transported over to Bill C-27.

This insight provides a summary of the key details of Bill C-27, including highlights of certain new provisions (compared to C-11).

1. **Penalties for non-compliance**

Organizations guilty of an indictable offence are liable to a fine of up to 5% of global revenue or CA$25 million, whichever is greater. There are administrative monetary penalties of up to 3% of global revenue or CA$10 million for other select violations of the *Consumer Privacy Protection Act* (CPPA).

What's new

The administrative monetary penalties (AMPs) apply to a greater number of provisions, which now include contraventions related to: establishment and implementation of a privacy management program, failure to ensure equivalent protection for personal information transferred to a service provider, failure to adequately specify purpose, consent, breach notification obligations on a service provider, and transparency.

Provisions attracting AMPs in Bill C-11 versus C-27			
C-11		C-27	
		s. 9(1)	Requirement to have implement a privacy management program including policies, practices, and procedures.
		s. 11(1)	Requirement to ensure service providers provide a level of protection equivalent to that which the

Provisions attracting AMPs in Bill C-11 versus C-27			
C-11		C-27	
			transferring organization is required to provide.
		s. 12(3)	Requirement to determine at or before the time of the collection each of the purposes for which the personal information is to be collected, used, or disclosed, and record those purposes.
		s. 12(4)	For any new purpose, the organization must record that new purpose before using or disclosing that information for the new purpose.
s. 13	Requirement that collection be limited to only the personal information that is necessary for the purposes determined and recorded.	s. 13	No change.
s. 14(1)	Prohibition against any use or disclose of personal information for a purpose other than a purpose determined and recorded, unless valid consent is obtained.	s. 14(1)	No change.
		s. 15(1)	Requirement that an organization must obtain an individual's valid consent for the collection, use, or disclosure of the individual's personal information, unless an exception applies.
s. 15(5)	Prohibition against an organization requiring consent as a condition of the supply of a product or service (beyond what is necessary to provide the product or service).	s. 15(7)	Numbering change.
s. 16	Prohibition against using false or misleading information or using deceptive or misleading practices to obtain consent.	s. 16	No change.
		s. 17(2)	Requirement that upon receiving a request to withdraw consent, the organization must inform the individual of the consequences of the withdrawal of their consent and, as soon as feasible after that, cease the collection, use, or disclosure of the individual's personal information.
s. 53	Prohibition against retaining personal information longer than necessary to fulfill purposes, or comply with law, plus an obligation to dispose of the information as soon as feasible after that period.	s. 53	No change.
s. 55(1)	Requirement to dispose of an individual's personal information on request, subject to exceptions.	s. 55(1)	Concept similar, with some wording changes.
s. 55(3)	Requirement to ensure disposal requests are communicated to, and carried out by, any service providers. /td>	s. 55(4)	Numbering change.

Provisions attracting AMPs in Bill C-11 versus C-27			
C-11		C-27	
s. 57(1)	Requirement that an organization protect personal information through physical, organizational, and technological security safeguards proportionate to the sensitivity of the information.	s. 57(1)	No change.
s. 58(1)	Requirement to report a breach to the Commissioner if it creates a real risk of significant harm.	s. 58(1)	No change.
s. 58(3)	Requirement to notify affected individuals of a breach, if it creates a real risk of significant harm.	s. 58(3)	No change.
		s. 61	Requirement that a service provider which determines that any breach of security safeguards has occurred must notify the organization that controls the personal information.
		s. 62(1)	Requirement to make readily available, in plain language, information that explains the organization's privacy policies and practices.

Both bills set out factors that the Commissioner must take into account when recommending a penalty. The factors were updated under C-27 to now include evidence that the organization exercised due diligence to avoid the contravention and reasonable efforts to mitigate or reverse the contravention's effects, providing organizations with additional avenues to attempt to limit penalties, and heightening the importance of a robust privacy compliance program.

2. **Privacy Commissioner –Powers**

The Office of the Privacy Commissioner of Canada (OPC) would oversee compliance with the CPPA. Along with other authorities, the Commissioner would have order making authority and the ability to make recommendations to a newly created Data Protection Tribunal regarding penalties.

3. **The Data Protection Tribunal**

The tribunal structure proposed in Bill C-11 to enforce the CPPA has been reintroduced in Bill C-27. Under the proposed regime, the federal Privacy Commissioner would have the power to recommend penalties, but the Tribunal may substitute its own decision.

The Tribunal will also be tasked with reviewing the Commissioner's orders. A decision of the Tribunal is final and binding, and, except for judicial review under *the Federal Courts Act*, is not subject to appeal or to review by any court.

What's new

The powers of the Tribunal have been elevated and are now equivalent to those of a superior court of record. Any decision of the Tribunal may be made an order of the Federal Court or of any superior court and is enforceable in the same manner as an order of the court.

4. **Private right of action**

The proposed legislation reintroduces the private right of action for contraventions of the CPPA where the

Commissioner or Tribunal has made a finding.

5. **Balanced purpose statement**

There is an explicit purpose statement in both Bill C-11 and Bill C-27, with the purpose of the CPPA being to establish rules to govern the protection of personal information in a manner that balances the right to privacy and the need for organizations to collect, use, or disclosure personal information. The balancing language in the purpose section of the CPPA is substantially similar to PIPEDA.

What's new

Bill C-27, which will establish three new statutes, also includes a lengthy preamble. The text references the aim of establishing "a regulatory framework that supports and protects Canadian norms and values, including the right of privacy." However, the preamble does not appear to expressly establish privacy as a human right in the Act. Recall that the recently departed Privacy Commissioner strongly advocated for a rights based framework, to shape the interpretation and application of the statute.

In addition, under Bill C-27, the Privacy Commissioner now must take into account certain factors when it exercises its powers, including the "purpose of this Act." This explicit requirement may provide a bulwark against the Privacy Commissioner unilaterally interpreting the Act that privileges a human rights approach.

6. **Consent-based regime**

The legal framework of Bill C-27 remains designed around a requirement that consent be obtained for the collection, use, and disclosure of personal information, unless one of the listed exceptions to consent applies. These exceptions include:

- Transfers to service providers.
- Use of personal information for internal research, analysis and development, provided the information is de-identified.
- Defined business activities if a reasonable person would expect the collection or use for such an activity; and the personal information is not collected or used for the purpose of influencing the individual's behaviour or decisions.

What's new

The concept of legitimate interests has been added as an exception to consent, where the legitimate interest outweighs any potential adverse effect on the individual. Bill C-27 brings needed clarity to the concept of legitimate interests, which was vaguely introduced in C-11 under the Business Activities provisions. Organizations relying on the legitimate interest exception will be required to complete a privacy impact assessment and to provide copies of the assessment to the Commissioner on demand.

7. **Sensitivity**

The sensitivity of personal information must be factored into the determination of whether the purposes of collection, use, and disclosure are appropriate, the form of consent, and security safeguards.

What's new

Organizations must take into account the sensitivity of personal information when determining retention periods, and transparency regarding the established retention policies.

8. **Children's privacy –** ***All NEW***

Bill C-27 includes the following new protections related to children's privacy:

- A minor's personal information is defined as being sensitive.
- Parents/guardians are authorized to exercise the rights and recourse under the CPPA on behalf of their child (including consent), however the child will have an opportunity to object to their parents authorizations if they are capable of doing so. The CPPA does not establish an age threshold as seen in other jurisdictions.
- Children are granted more expansive rights to have their personal information deleted (under the Disposal provisions).

9. **De-identification and anonymization**

Bill C-27 clarifies the approach taken under Bill C-11, which conflated de-identified and anonymized information and made them both subject to privacy legislation, a position that was out of step with the global approach to the issues. Businesses pushed back on these provisions of C-11, raising concerns that such an approach would stifle technological innovation and impact Canada's participation in the digital economy. The drafters of Bill C-27 appear to have listened, and the new definitions and approach largely align with global standards.

What's new

The de-identification provisions have been clarified. De-identify in Bill C-27 means to modify personal information so that an individual cannot be *directly* identified from it, though a risk of the individual being identified remains.

Bill C-27 also contains a definition for anonymize, which is 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. Helpfully, Bill C-27 also explicitly states that anonymized information falls outside the scope of the CPPA.

10. **Disposal**

Individuals have a right to request disposal of their personal information, with certain limited exceptions.

What's new

The right of disposal has arguably been broadened under Bill C-27. Under Bill C-11, the right to disposal applied to personal information "collected from" an individual, whereas under Bill C-27, the scope includes all personal information that is "under an organization's control." There are six exceptions, including where:

- The disposal would have undue adverse impact on the accuracy or integrity of information that is necessary to the ongoing provision of a product or service; or
- The personal information is scheduled to be disposed of in accordance with a retention policy, and the organization informs the individual of the remaining period of time for which it will be retained. Both of these exceptions apply broadly except in the case of minors.

11. **Algorithmic transparency**

Upon request organizations would be required to provide explanations of the prediction, recommendation, or decision made about an individual by automated means.

What's new

An individual's right to explanation has been narrowed to decisions about the individual that "could have a significant impact on them." This materiality threshold is more in line with global standards.

While the scope is narrower, there are new requirements for the elements to be included in an explanation. Namely, it 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 or principal factors that led to the prediction, recommendation, or decision. There is some alignment with Québec's Bill 64 explainability obligations.

12. **Security safeguards**

An organization is required to protect personal information through physical, organizational, and technological security safeguards, and the level of protection must be proportionate to the sensitivity of the information.

What's new

Bill C-27 expands the scope of the security safeguards and would require "reasonable measures to authenticate the identity of the individual to whom the personal information relates." As drafted, this has the potential to introduce significant friction into business operations.

13. **Artificial Intelligence and Data Act - *All NEW***

The new AI and Data Act (**AI Act**) creates a framework for high-impact AI systems. Dentons will be providing a detailed analysis in the coming weeks, but we summarize the basic elements here.

The purposes of the AI Act are to:

- Regulate international and interprovincial trade and commerce in artificial intelligence systems by establishing common requirements, applicable across Canada, for the design, development, and use of those systems; and
- Prohibit certain conduct in relation to artificial intelligence systems that may result in serious harm to individuals or harm to their interests.

An artificial intelligence system is defined as "a technological system that, autonomously or partly autonomously, processes data related to human activities through the use of a genetic algorithm, a neural network, machine learning or another technique in order to generate content or make decisions, recommendations or predictions."

The requirements, designed to address the risk of bias and harm, apply to "high-impact" systems, though the term is not defined in the proposed legislation (it is left to regulation).

The proposed legislation would create an Artificial Intelligence Data Commissioner housed within a ministry, who would assist with enforcement. The minister may delegate to the Commissioner information sharing powers and order making authority, including to request records, require organizations to conduct audits, take action to address issues, and cease operation of certain high-impact systems where there is a "serious risk of imminent harm".

The AI Act provides for administrative monetary penalties for violations of the regulations and fines for violations of the requirements set out in the Act.

14. **Coming into force**

Bill C-27 is not expected to advance in the House before it rises for the summer on June 23. The Bill will need to go to committee; Bill C-11 went to the Committee on Access to Information, Privacy and Ethics (ETHI) (with calls that it should have gone to the Standing Committee on Industry and Technology (INDU)). This will likely be a point of contention with Bill C-27 as well, with businesses pressuring the government to send it to INDU (or both committees), especially in light of incoming Privacy Commissioner Philippe Dufresne's long background in human rights adjudication.

In its technical briefing, Innovation, Science and Economic Development Canada indicated that once the Bill is

passed, there would be a “significant” amount of time provided for organizations to become compliant.

If you have any questions about Bill C-27, please feel free to reach out to a member of Dentons Canada’s Privacy and Cybersecurity group.

Your Key Contacts

Kirsten Thompson
Partner, Toronto
D +1 416 863 4362
kirsten.thompson@dentons.com

Chantal Bernier
Of Counsel, Ottawa
D +1 613 783 9684
chantal.bernier@dentons.com

Tom A. Sides
Partner, Edmonton
D +1 780 423 7138
tom.sides@dentons.com

Kelly Osaka
Partner, Calgary
D +1 403 268 3017
kelly.osaka@dentons.com

Chloe A. Snider
Partner, Toronto
D +1 416 863 4674
chloe.snider@dentons.com

Julie Facchin
Counsel, Vancouver
D +1 604 691 6465
julie.facchin@dentons.com

Alexandra Quigley
Senior Associate, Montréal
D +1 514 878 5856
Alexandra.quigley@dentons.com