IAB Canada Policy Brief

C-27

Federal Privacy Legislation

An Act to support and promote electronic commerce by protecting personal information that is collected, used, or disclosed during commercial activities. Provides clear rules around data collection and use practices, consent, exceptions to consent, risk mitigation, and more significant documentation of internal processes. Strengthens protections for minors against improper use of their data. Once passed, this law will replace the *Personal Information Protection and Electronic Documents Act* (PIPEDA). This Act is a part of the Digital Charter Implementation that also includes the Data Protection Tribunal Act and the Artificial Intelligence and Data Act (AIDA)

Sponsor: Minister of Innovation Science and Industry
Current Status: Debated in Senate at second reading on March 7, 2023 (House of Commons). Expected to come back in discussions in early Fall, 2023

Key changes impacting business include:

1. A new **enforcement regime** with severe **financial penalties**, a **private right of action**, **and order making power** for the Privacy Commissioner
    - Enables broad audit and order-making powers, and the ability for the Commissioner to make recommendations to the Tribunal for the imposition of significant administrative monetary penalties (AMPs)
    - 'AMPs' of up to CAD 10 million or 3% of the organisation's global gross revenues, whichever is higher, with most egregious violations would constitute offences punishable, upon prosecution, with a fine of up to CAD 25 million or 5% of the organisation's global gross revenues.
    - Introduction of a new private right of action by which an individual 'affected' by a contravention may (within two years) bring a claim against the organisation for damages for loss or injury suffered because of the contravention.

2. A **re-enforcement of consent** (especially express consent) as the **primary authority** for organizations to **process personal information** as well as **more prescriptive consent requirements.**

3. **Clarifications** and additional "**exceptions to consent**" authorities for use and disclosure of personal information **including** things such as **standard business activities** and for **legitimate interests.**
    - Allows for the collection and use of personal information without consent for certain business activities where it would reasonably be expected to be collected or used to provide the service requested, for security purposes, for safety, or for other prescribed activities. Also includes a 'legitimate interest' exception to consent for collection and use, but it requires an organisation to first identify any potential adverse effects on the individual that is likely to result from the collection or use,

mitigate or eliminate them, and finally weigh whether the legitimate interest outweighs any adverse effects.

The list of business activities covered by this consent exception are activities:

- Necessary to provide or deliver a product or service that the individual has requested from the organization.
- Carried out in the exercise of due diligence to prevent or reduce the organization's commercial risk.
- Necessary for the organization's information, system, or network security and for the safety of a product or service that the organization provides or delivers.
- During which obtaining the individual's consent would be impracticable because the organization does not have a direct relationship with the individual, or any other prescribed activity.
- Socially beneficial purposes and research and statistics

4. **Provisions** relating to **de-identified** and **anonymized** information.
    - CCPA defines to anonymise as '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'. It does not regulate anonymous data because, by definition, there is no reasonable prospect of re-identification.
    - To de-identify data means 'to modify personal information so that an individual cannot be directly identified from it, though a risk of the individual being identified remains'. The CPPA does regulate de-identified data and generally prohibits attempts to re-identify it and it allows for organisations to use an individual's personal information without their consent to de-identify their data.

5. **More prescriptive** and **strengthened accountability requirements.**
    - Organizations are required to keep records of consents and the purposes for which it collects, uses, and discloses data. To use data for a new purpose, a separate consent, must be obtained and documented in an accessible form in case of audit.

6. **Clarification** of the **obligations** of **service providers**
    - CCPA defines a service provider as "an organization, including a parent corporation, subsidiary, affiliate, contractor or subcontractor, which provides services for or on behalf of another organization to assist the organization in fulfilling its purpose" (s. 2). Section 19 of the CPPA will expressly permit organizations to transfer personal information to a third-party service provider without knowledge or consent.

The following principles that apply to outsourcing are clarified:

- personal information collected, used, or disclosed on behalf of an organization by a service provider is deemed to be under the control of the organization (not the service provider) if the organization determines the purposes of collection, use or disclosure (s. 7(2)).

- the CPPA imposes accountability on an organization that transfers personal information to a third-party service provider to ensure (by contract or otherwise) that the service provider provides similar protection over that personal information (s. 11(1)).
- Obligations set out in the CPPA do not apply to a service provider to the extent that an organization transfers personal information to it for processing. If the service provider collects, uses, or discloses personal information for any other purpose, then Part 1 of the CPPA applies (s. 11(2)).
- If an organization disposes of personal information upon request by an individual, the CPPA requires the organization to notify and confirm its service providers do the same and the CPPA also imposes notification obligations on a service provider that suffers a data breach.

7. A new focus on the **protection of minors**
    - The law considers minors' personal data to be sensitive. and requires businesses to obtain explicit consent to collect, use, and disclose personal information of minor. Parents or guardians can exercise the rights (including consent) on behalf of their child, but the child can object to their authorization. Children also have the right to have their personal data deleted.

8. **Statutory recognition** of **codes of practice** and **certification programs**
    - In addition to the requirement for a privacy management program the CPPA allows private organisations to establish a 'code' and internal certification programs for complying with the CPPA, which the Privacy Commissioner will approve. Once approved, this 'code' will effectively establish the organisation's legal compliance obligations.

9. New **statutory right of disposal and data mobility rights**
    - Consumers can require an organisation to transfer their data to another organisation, provided that the organisations are connected to a 'data mobility framework'. An individual can also request that an organisation dispose of their information; notably, disposal includes deletion and rendering the data anonymous.

10. New **Algorithmic transparency requirements**
    - The CPPA requires organisations to provide in their privacy policy a general account of the organisation's use of any automated decision system to make 'predictions, recommendations, or decisions about individuals that could have a significant impact on them'. On request by the individual, the organisation must provide them with an explanation of the prediction, recommendation, or decision. 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 or principal factors that led to the prediction, recommendation, or decision.

Implications for Digital Advertising Industry

- Increased need for IAB Canada members to evaluate partners in the supply chain ensuring they are aligned on privacy practice and data protection procedures.
- Time to up reliance on use of tested technology and practices that enable up front transparency, disclosures, consent collection and receipts to ensure the legal collection of data and use for digital advertising.
- Privacy is making its way at the core of all discussions – creative and strategic – real need for understanding requirements from a broader perspective.
- Continued discussions on the efficiency of working to the highest-level requirements – eliminating financial waste and tech debt.

IAB Canada Activity

- Continued dialogue with government stakeholders/policy makers at ISED and OPC – will testify at Senate once Bill reaches that stage as well as continue to feed into regulations and guidance on behalf of industry.
- Participating in cross-industry dialogue on the privacy file representing the online advertising sector
- Working towards attaining approval of TCF Canada as a recognized framework under CCPA

Further Reading - Full content of the Bill