大成 DENTONS

# Canada's Bill C-27: What it means for children's privacy and the impact on business

Grow | **Protect** | Operate | Finance

Bill C-27's proposed *Consumer Privacy Protection Act* (CPPA) includes new protections for minors by requiring a higher standard of diligence and protection in respect to the collection and processing of their personal information. Legislators in Canada are clearly following international trends with respect to the protection of children's personal information, and organizations that operate in sectors interacting with children's personal information on any level will need to pay close attention. Increasing regulatory scrutiny of the handling of children's personal information, and an upswing in class actions related to the same issue, have created a material change in the risk environment for these businesses.

**Background**

Bill C-27, currently in second reading, proposes to overhaul Canada's current federal private-sector privacy law (a summary of Bill C-27 can be found here). Part 1 of the new Bill would enact the CPPA as an updated framework to govern the protection of personal information while taking into account businesses' need to collect, use or disclose personal information. While much of Bill C-27 refines or builds out existing privacy protections found in PIPEDA, it also contains some wholly new provisions. Among these new provisions are new privacy requirements in respect of children's personal information (**cPI**).

**We examine:**

1. The amendments proposed in the CPPA as they relate specifically to the protection of cPI;
2. How the proposed protections compare to other child protection frameworks; and
3. Potential impact on businesses and the practical steps that organizations can take to ready themselves.

## 1. The CPPA's children's privacy proposals

***Treatment of cPI as "sensitive information"***

Personal information that is "sensitive" requires heightened privacy protections and will generally require express consent for its collection, use or disclosure. Under PIPEDA, determining what information may be sensitive has posed a challenge for businesses, as any personal information can be sensitive depending on the context; there is no definitive list featuring types/categories of sensitive personal information like in the European Union's *General Data Protection Regulation* (GDPR). A recent Interpretation Bulletin from the Office of the Privacy Commissioner of Canada (**OPC**) attempted to provide some clarity by stating that sensitive personal information "includes health and financial data, ethnic and racial origins, political opinions, genetic and biometric data, an individual's sex life

or sexual orientation, and religious or philosophical beliefs"; however, the contextual approach remains valid for all other personal information. There is no mention of children, cPI, or the personal information of minors in this Bulletin.

The CPPA largely continues this approach and does not define "sensitive personal information" – with the notable exception of cPI. In the CPPA, a minor's personal information is now the only prescriptive category that is expressly defined as being "sensitive information."

This designation of cPI as "sensitive" means it attracts heightened protections, positive obligations for deletion, a requirement for express consent for its collection, use or disclosure, and a host of other obligations.

***Form of consent***

Both PIPEDA and the CPPA state that consent must be expressly obtained unless it is appropriate to rely on an individual's implied consent, taking into account "the reasonable expectations of the individual and the sensitivity of the personal information." While there is no explicit requirement in either PIPEDA or the CPPA for express consent to process cPI, by designating cPI as sensitive it will be difficult to use any form of consent other than express. Organizations should interpret the requirement to consider the sensitivity as requiring express consent.

This *de facto* requirement for express consent will likely require businesses to review (and revise) their consent processes and language.

***A child's ability to provide consent***

The validity of consent provided by a minor is always an issue in law. Under the CPPA, parents, guardians or tutors would be authorized (though not required) to exercise the rights and recourses under the Act on behalf of the child, including the ability to consent on the minor's behalf. The CPPA does not provide an age threshold below which a minor is not deemed to be able to provide consent. Importantly, minors are permitted to exercise control if they wish to, and they are "capable of doing so." While this proposal is in line with the reality that mature teenagers currently interact freely online without the need for parental involvement, businesses may find it difficult to know when (and whose) consent is valid for their purposes. If a parent purports to withdraw their child's consent to a social media app but the child objects, a business may be in the uncomfortable position of having to determine a minor's capacity to consent.

There is no guidance in the CPPA regarding the evaluation of capacity. Ontario's *Personal Health Information Act* provides that an individual is capable of consenting to the processing of personal health information if the individual is able:

- to understand the information that is relevant to deciding whether to consent to the collection, use or disclosure, as the case may be; and
- to appreciate the reasonably foreseeable consequences of giving, not giving, withholding or withdrawing the consent.

This may provide a helpful framework for evaluating capacity if one is not advanced as Bill C-27 moves through the legislative process. Either way, the onus will be on organizations to take into account the maturity level of their audience when determining their consent processes.

Organizations appear to be able to impose their own age-gating requirements on top of the requirements of the CPPA. For instance, it is open to an organization to require (as a term of use or contractual term) that users of their products or services be X years old and that those under X years of age must have consent provided by a parent, guardian or tutor. This may be one way to minimize a potential clash of consents.

***Appropriate purposes***

Under the CPPA, there is an overarching requirement that an organization can only collect, use or disclose personal information for purposes that a reasonable person would consider appropriate in the circumstances. There are various factors that must be taken into account, including the sensitivity of the personal information, which as described above, links this requirement to the acceptable treatment of cPI.

The OPC previously published a guidance document in which it developed a list of "no-go zones" or inappropriate data practices based on a substantially similar provision in PIPEDA (see *Guidance on inappropriate data practices: Interpretation and application of subsection 5(3)*). There is room to broadly interpret protections for children under this provision and we expect to see further regulatory guidance outlining activities that will always be inappropriate.

For example, the federal Privacy Commissioner previously found that pre-set user privacy settings to 'visible to all' by a social networking site for youth was inappropriate (see PIPEDA Report of Findings #2012-001). Although this Finding was based on the interpretation of PIPEDA, it is likely that under the proposed CPPA, operators of apps or other platforms which minors may subscribe to will need to ensure that settings are set to private by default.

***Plain language requirements***

The CPPA requires the disclosure of certain information in order for consent to be considered valid. It further requires that the information be presented in plain language that would be understood by the targeted audience. Companies which process or collect cPI will need to think about elements of their business operations such as the contents of their privacy notices, which will need to be adapted to the age of their audience to ensure that the terms of any collection are conveyed in an age-appropriate manner and will be clearly understood.

Businesses that have multiple target audiences (e.g., youth and adult services) may need to have two separate versions of their privacy policies.

***Disposing of personal information***

Under the CPPA, if an organization receives a written request from an individual to dispose of their personal information that is under the organization's control, the organization must, as soon as possible, dispose of the information, if: (i) the information was collected, used or disclosed in breach of the Act; (ii) consent is withdrawn; or (iii) the information is no longer necessary for the continued provision of a product or service requested by the individual.

The organization may refuse a request to dispose of this personal information in certain situations, including where:

- The disposal of the information would have an undue adverse impact on the accuracy or integrity of information that is necessary to the ongoing provision of a product or service to the individual in question; and
- If the information is scheduled to be disposed of in accordance with the organization's information retention policy and the organization informs the individual of the remaining period of time for which the information will be retained.

However, these exceptions to disposal will not apply if the personal information in question is "in relation to" a minor. This right applies to information collected not only directly from the individual, but to personal information collected from all sources as long as it is "under the organization's control." As a result, app, platform and site developers and operators will need to ensure that disposal is front of mind and be prepared for this broader right for children under the CPPA.

***Retention***

Under the CPPA, organizations would be required to take into account the sensitivity of the information when setting retention periods. Therefore, businesses should be particularly mindful when setting retention schedules for cPI and retain it for the minimum demonstrably necessary period. Note that the CPPA would also introduce a new requirement to make available retention periods that apply to sensitive personal information. As a result, this requirement will apply to cPI.

## 2. Comparisons

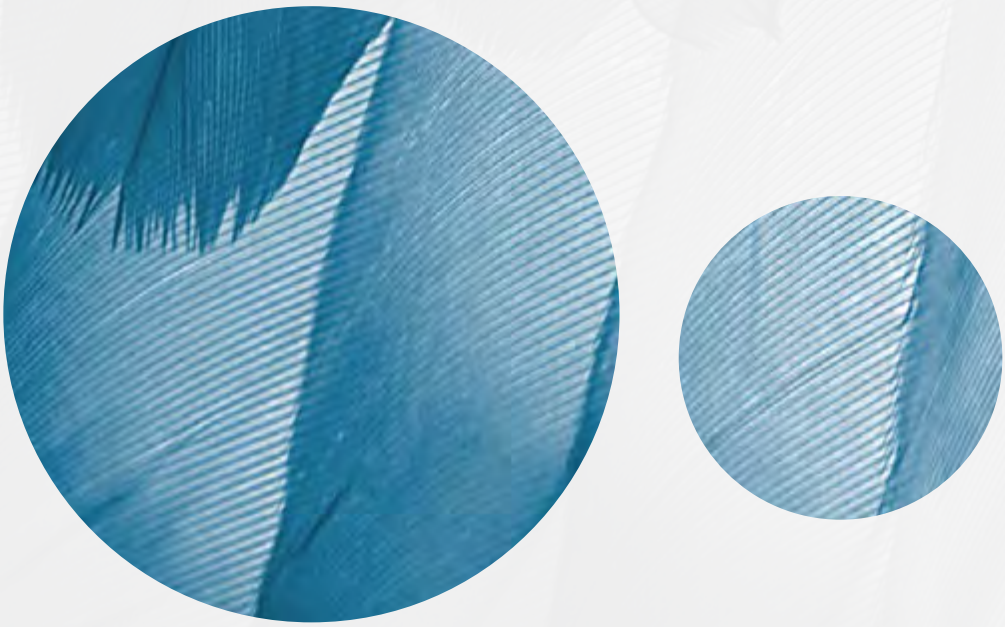
### *Definition of a "minor"*

As indicated above, the CPPA does not define a "minor" or provide a specific age threshold for the concept of cPI. Generally speaking, a minor is a person who has not yet reached the age of majority, the age at which a person is considered to be an adult legally, and in Canada it is normally determined by province of residence. A person may be a minor in one province and an adult in another, which could create challenges for organizations trying to interpret and apply the CPPA provisions.

"Minor" or "child" may also be defined in the applicable statute itself. For instance, note the following age thresholds:

| Instrument | Age threshold |
|---|---|
| Québec Bill 64 (introducing new requirements into the *Act respecting the protection of personal information in the private sector*) | Under 14 |
| Québec *Consumer Protection Act* | Under 13 |
| CPPA | *Undefined* |
| Broadcast Code for Advertising to Children (Children's Code) | Under 12 |
| OPC guidance (*see Collecting from kids? Ten tips for services aimed at children and youth*) | Under 13 ("youth" are under 18) |
| GDPR | Under 16 (or 13) (member states can establish a lower age, provided that the age is not below 13). |
| UK Age-Appropriate Design Code | Under 18 |
| UN Convention on the Rights of a Child | Under 18 |
| Children's Online Privacy Protection Rule (COPPA) - USA | Under 13 |

Who is or is not a minor will likely be a contested area of law, and we expect that the proposed Tribunal will interpret who is considered a "minor."



### *Comparison of special children's requirements within Canada*

Organizations should consider the interplay between various requirements related to the treatment of cPI in Canada. In Québec, the *Consumer Protection Act* includes limitations regarding advertising directed to minors and Bill 64 introduced new requirements related to parental consent and de-indexing. The interplay between Québec's legislation and the CPPA will set parameters on the processing of cPI in Canada, and likely inform how organizations manage cPI to avoid a patchwork approach to compliance.

| | **Québec Bill 64 updates to the *Act respecting the protection of personal information in the private sector*** | **Québec *Consumer Protection Act*** | **CPPA** |
|---|---|---|---|
| **Main requirements** | The personal information concerning a minor under 14 years of age may not be collected from them without the consent of the person having parental authority or of the tutor, unless collecting the information is clearly for the minor's benefit. | Prohibits the use of commercial advertising directed at persons under thirteen years of age, subject to limited exceptions. | Parents/guardians are authorized to exercise the rights and recourse under the CPPA on behalf of a minor (including consent), however the minor may object to their parents authorizations if they are capable of doing so. |
| **Children's Rights** | De-Indexing - As of September 2023, Bill 64 gives individuals a right to request that a hyperlink attached to their name be de-indexed (subject to a number of exceptions). One of the criteria for evaluating de-indexing requests is if the information concerns the person while they were a minor. | | Deletion - Minors would be granted more expansive rights to have their personal information deleted under the disposal provisions. |

### *International approach*

Canada is clearly following the trend set by other jurisdictions within and outside of Canada that have adopted more stringent requirements in regards to cPI. Below, we summarize key requirements from some international instruments in this area, which likely influenced the changes to the CPPA and may pave the way for the implementation of protections in the future.

- **GDPR requirements**

The GDPR's preamble notes that children merit specific protection with regard to their personal data, as they may be less aware of the risks, consequences and safeguards concerned and their rights in relation to the processing of personal data. There are parental consent requirements under the GDPR, as well, the interests and fundamental rights and freedoms of a child are given enhanced consideration when assessing whether to process personal information on the basis of legitimate interests.

Similar to the requirements in the CPPA, data controllers also must make reasonable efforts to verify that consent is given or authorized by the parent or guardian, taking into consideration available technology.

- **Codes**

The UK's Age-Appropriate Design Code sets out that products and services in scope of the Code must consider the privacy and protection of children, by design and default, and that if there is a conflict between the service and child, the child's best

interest must be paramount. This Code sets out specific protections for cPI in compliance with the provisions of the UK GDPR.

Since this Code was passed, companies have refined their privacy practices as they apply to children, for instance by choosing to disable direct messages between children and adults, and by applying filters that remove explicit content for all children under 18 by default.

It is clear as well, that the UK Information Commissioner is trying to encourage the adoption of the Code beyond the borders of the UK. In fact, California has just set a new standard in the US with the passage of the California Age Appropriate Design Code Bill, based on the UK model.

- **New EU regulation**

Finally, the EU is taking further steps to protect children online with its Digital Services Act which will ban platforms from delivering targeted advertisement to children.

## 3. Practical steps in preparation for CPPA compliance

Organizations with apps, platforms, websites, and other products and services accessed or used by minors should consider default privacy protections and settings, including:

- Clearly setting out easy-to-understand terms and conditions in privacy policies and practices, with the retention periods applicable to any personal information relating to a minor (now considered as "sensitive information") also being made available.
- Ensuring express/opt-in consent is obtained, either by a minor who is able to provide meaningful consent, or by their parent, guardian or tutor.
- Implementing technical means in order to dispose of cPI in a timely manner upon request (and subject to the exceptions).
- Implementing means by which such requests for disposal of cPI can be passed on to service providers (and confirmed).
- Consider introducing age-gating mechanisms and/or age validation measures if they are not already in place.
- Develop an approach to handle the parent/minor consent clash.
- Review the various competing definitions of "minor" and make internal decisions as to how best to address this, having regard to the types of cPI collected (e.g., name and address versus comprehensive user profile), the age of the minor (e.g., 13 versus 17), and the inherent sensitivity of the cPI (e.g., a platform for gaming versus a platform connecting children who have cancer).
- Develop compliance measures in respect of targeted advertisements to minors, or prohibit such targeting altogether.
- Be able to identify cPI, and handle it accordingly, including minimal retention periods and routine secure disposal.

If you have any questions about the Bill, the legislative process or opportunities to make a submission, please feel free to reach out to a member of Dentons Canada's Privacy and Cybersecurity Group.

*For more information about Dentons' data expertise and how we can help, please see our unique Dentons Data suite of data solutions for every business, including enterprise privacy audits, privacy program reviews and implementation, data mapping and gap analysis, and training in respect of personal information.*

Authored by Kirsten Thompson, Danielle Dudelzak, and Jen Rees-Jones

## ABOUT DENTONS

Dentons is designed to be different. As the world's largest law firm with 20,000 professionals in over 200 locations in more than 80 countries, we can help you grow, protect, operate and finance your business. Our polycentric and purpose-driven approach, together with our commitment to inclusion, diversity, equity and ESG, ensures we challenge the status quo to stay focused on what matters most to you.

**www.dentons.com**



CSBrand-97637-Protection of children's personal information in Canada-04 — 28/09/2022