Michael J. S. Beauvais, BA, BA, BCL/JD, MSc
Doctoral Candidate, Faculty of Law, University of Toronto
Graduate Fellow, Schwartz Reisman Institute for Technology and Society
Affiliate, Information Law Institute, New York University School of Law

Leslie Regan Shade, PhD
Professor, Faculty of Information, University of Toronto
Faculty Affiliate, Schwartz Reisman Institute for Technology and Society

October 30, 2023

Mr. Joël Lightbound, M.P.
Chair, Standing Committee on Industry and Technology
House of Commons
Ottawa ON K1A 0A6

RE: Submission to the Standing Committee on Industry and Technology Study of Bill C-27, The Digital Charter Implementation Act, 2022[1]

Dear Mr. Lightbound,

As scholars in children's privacy and data protection, we are writing to you in response to the Standing Committee on Industry and Technology's study of Bill C-27. In what follows, we provide 10 recommendations with accompanying rationales with respect to the provisions related to minors in the proposed *Consumer Privacy Protection Act* (CPPA). These recommendations will clarify and strengthen the provisions dealing with minors.

The CPPA implicates a broad swath of interests of minors, parents, and others. When we speak about privacy and data protection for youth, issues of freedom of expression for adults and minors, access to information, and participation in society more broadly are also implicated. With this in mind, we want to underscore the need to recognize and balance these concerns in a context-sensitive manner. For example, youth can be excluded from platforms because companies do not want to comply with their obligations under privacy laws.[2] Some of these platforms form a public square and are an essential communication space for civic participation, education, entertainment, and more.

Digital privacy for children and young people is important. This is especially the case as increasingly their social lives, private experiences and access to education and future careers involve the processing of personal information by powerful platform companies and third parties whose business model is reliant on mining their personal information through surveillance, targeted advertising, and algorithmic

[1] We are immensely grateful for the support of David Baldridge, Policy Researcher, at the Schwartz Reisman Institue for Technology and Society in preparing this brief.

[2] See Chapter 5, "Privacy First, Safety Later" (pp 174-215), in Grimes, Sara M, *Digital Playgrounds: The Hidden Politics of Children's Online Play Spaces, Virtual Worlds, and Connected Games* (Toronto: University of Toronto Press, 2021).

decision-making to influence their choices.[3] It is thus paramount that we situate privacy as a key element of digital inclusion and that we bring forward the perspectives and voices of diverse Canadian youth into privacy law and policy to highlight how the "intersectional social location of youth shapes their online experiences."[4]

In Canada youth privacy is increasingly recognized as a strategic priority among information and privacy commissioners. The Office of the Privacy Commissioner's 2022-2023 Annual Report to Parliament noted the importance of "protecting children's privacy so that they can benefit from technology and be active online safely and free from fear that they may be targeted, manipulated, or harmed as a result."[5] Children's privacy is also a strategic priority for the Information and Privacy Commissioner of Ontario; they recommend strengthening access and privacy rights for children through digital literacy while calling for accountability from institutions.[6]

And, a recent resolution of the Federal, Provincial and Territorial Privacy Commissioners and Ombuds with Responsibility for Privacy Oversight called on their respective governments to "put the best interests of young people first" through a variety of means: promoting privacy rights for children, protection from commercial exploitation wherein personal information can negatively influence behaviour or cause harm, requiring private sector organizations that collect, use and disclose personal information of young people to be transparent about their practices, implement strong safeguards and enhance access to effective remedies for children, and reviewing, amending or adopting privacy legislation to align with international policy and legal instruments on children's privacy rights.[7]

While we believe that taking children's interests seriously is a good onto itself, it is important to note that Canada's maintenance of an adequacy decision under the *General Data Protection Regulation* (GDPR) from the European Commission is likely to require robust rules for children's personal information. Adequacy under the GDPR is a markedly more demanding process than what happened for

---

[3] Automated decision-making (ADM) is the process of making decisions via automated methods, such as AI, without human involvement. ADM is central to digital services that children use and can negatively shape their health and well-being through a relentless valorization of popularity ('friend' recommendations), persuasive design ('nudges'), misinformation, and exposure to harmful material. See 5Rights Foundation, Shedding Light on AI: A Framework for Algorithmic Insight, June 2022, https://5rightsfoundation.com/Shedding-light-on-AI---a-framework-for-algorithmic-oversight.pdf.

[4] Shade, Leslie Regan et al, "Framing the Challenges of Digital Inclusion for Young Canadians" in Elizabeth Dubois & Florian Martin-Bariteau, eds, *Citizenship in a Connected Canada: A Research and Policy Agenda* (Ottawa, ON: University of Ottawa Press / Les Presses de l'Université d'Ottawa, 2020) 57.

[5] *2022-2023 Annual Report to Parliament on the Privacy Act and the Personal Information Protection and Electronic Documents Act* (Ottawa, ON: Office of the Privacy Commissioner of Canada, 2023) https://www.priv.gc.ca/media/5996/annual-report-2022-23.pdf.

[6] Information and Privacy Commissioner of Ontario, "IPC Strategic Priorities 2021-2025", online: *IPC* <https://www.ipc.on.ca/about-us/ipc-strategic-priorities-2021-2025-final-report/ipc-strategic-priorities-2021-2025/>.

[7] Resolution of the Federal, Provincial and Territorial Privacy Commissioners and Ombuds with Responsibility for Privacy Oversight, *Putting best interests of young people at the forefront of privacy and access to personal information*, (Quebec, QC, 2023) https://www.priv.gc.ca/en/about-the-opc/what-we-do/provincial-and-territorial-collaboration/joint-resolutions-with-provinces-and-territories/res_231005_01/.

the *Personal Information Protection and Electronic Documents Act* under the EU's previous regime, the *Data Protection Directive*.[8] The GDPR's provisions includes specific articles specifying privacy guarantees for children.[9] The GDPR's recitals, serving as an interpretive aid, buttress a child-friendly interpretation of the GDPR.[10] Robust guarantees for children's privacy, then, is as much a commercial issue as it is one of fundamental rights protections.

We have limited our recommendations to the most salient issues affecting the privacy of young people. Nevertheless, we want to highlight some important aspects of briefs already submitted to the Committee. We endorse Colin Bennett's point about the lack of international data transfer rules in the CPPA. Pertinent points related to the connection between privacy and equality, the impact of personal data collection, and use and disclosure for individual and collective rights have been raised by Jane Bailey, Jacquelyn Burkell and Brenda McPhail. We endorse their call for a robust individual informed consent model (IICM) and a more fulsome recognition and protection of group, collective, and community privacy and equality rights. UNICEF Canada has provided nine specific recommendations on children's privacy that we applaud, including conducting a Child Rights Impact Assessment, inclusion of best interests of the child as a guiding principle and the need to affirm the Government's commitment to universal access and developing digital rights literacy information. We endorse Kate Robertson's calls for better regulating consumer spyware and stalkerware apps through the CPPA. Finally, we endorse the call of Bannerman, et al. (in an incoming brief) for an intersectional analysis of Bill C-27.

We thank you for your consideration.

Sincerely,

Michael J. S. Beauvais and Leslie Regan Shade

[8] Case C-311/18, *Facebook Ireland and Schrems*, 2020 Court of Justice of the European Union; *Commission Implementing Decision (EU) 2019/419 of 23 January 2019 pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council on the adequate protection of personal data by Japan under the Act on the Protection of Personal Information*, OJ L 76/1 2019.

[9] The GDPR includes a specific regime for children's consent to the use of information society services (e.g., social media, video platforms) in article 8 and other child-centric provisions in articles 6, 12, 40, and 57. For an excellent commentary on these articles and the GDPR as a whole, see Kuner, Christopher, Lee Bygrave & Christopher Docksey, eds, *The EU General Data Protection Regulation (GDPR): A Commentary* (New York, Oxford: Oxford University Press, 2020).

[10] See recitals 38, 58, 65, 71, and 75 of the GDPR.

Recommendations

1. Expressly reference the best interests of the child

Recommendation: Insert provisions into ss. 2(2) and 5 of the CPPA that the best interests of the child will be a primary consideration for all matters affecting minors.

Rationale: The draft CPPA does not mention the best interests of the child. Nor do the proposed amendments in Minister Champagne's letter from October 20, 2023. This is surprising. The best interests of the child standard is a bedrock to issues involving law and minors. Incorporating the best interests of the child into legislation and policy is part of Canada's obligations as a party to the *Convention on the Rights of the Child*. Doing so ensures that decisions, including procedures and legal interpretations, bring forward children's best interests. The best interests of the child principle has three dimensions, each of which the CPPA implicates: a right, an interpretive principle, and a rule of procedure.[11] As a right, both individual minors and minors as a group have a right to have their best interests determined and be a primary consideration for any decisions affecting them. Combined with other children's rights, this guarantees that children's interests are at the forefront of decisions and policy. As an interpretive principle, it says that in cases of interpretive ambiguity, the interpretation that best serves the child's interests should be chosen. As a rule of procedure, it requires that a decision's impact on a minor be taken into consideration in the decision-making process.

The best interests of the child has been recognized through a resolution from federal, provincial, and territorial informational and privacy commissioners, and as Commissioner Dufresne recently noted, "Privacy laws should recognize the rights of the child, and the right to be a child. This means interpreting the privacy provisions in the legislation in a way that is consistent with the best interests of the child."[12] Indeed, the best interests principle is a pillar to the *Convention on the Rights of the Child* and to federal, provincial, and territorial laws that affect minors. Including the best interests principle expressly gives regulators and tribunals the opportunity to consider a child's best interests in determining matters under the CPPA. Given the wide range of interests that personal information implicates – from both individuals and organizations – including the best interests of the child standard ensures that the interpretation and enforcement of the CPPA brings children's interests to the forefront.

2. Treat privacy as a fundamental right

Recommendation: Include privacy's status as a fundamental right in the preamble and as an interpretive principle in s. 5 of the CPPA.

[11] United Nations Committee on the Rights of the Child. "General Comment No.14 (2013) on the Right of the Child to Have His or Her Best Interests Taken as a Primary Consideration (Art. 3, Para. 1)." United Nations Committee on the Rights of the Child, May 29, 2013. CRC/C/GC/14.

[12] Philippe Dufresne for the Office of the Privacy Commissioner of Canada, "Appearance before the Standing Committee on Access to Information, Privacy and Ethics on its study of the Use of Social Media Platforms for Data Harvesting and Unethical or Illicit Sharing of Personal Information with Foreign Entities", (25 October 2023), online: <https://priv.gc.ca/en/opc-actions-and-decisions/advice-to-parliament/2023/parl_20231025_02/>.

Rationale: All persons in Canada have a human right to privacy by virtue of Canada's ratification of the *International Covenant on Civil and Political Rights*.[13] Children furthermore have a right to privacy under the *Convention on the Rights of the Child*.[14] We endorse the proposed October 20, 2023 amendments from Minister Champagne to include the status of privacy as a fundamental right to the preamble and to s. 5 of the CPPA.

3. Define a minor

Recommendation: Define a minor, by referring to the relevant applicable territorial or provincial law of the minor's primary residence.

Rationale: The additional guarantees for minors in the CPPA should not end when that minor attains capacity or an age lower than that of majority. The proposals to define a minor from the Canadian Chamber of Commerce and Canadian Vehicle Manufacturers' Association as a natural person under the age of 14 means that in a highly datafied society, individuals between 14 and 18/19 lose the additional guarantees in the CPPA that support their agency and protection, such as a more robust right to data deletion and data security measures, before they attain the age of majority. Moreover, the slight variation for age of majority across Canada is not a new burden for organizations; they must already deal with the definition of a minor being either 18 or 19 in each province or territory.

4. Define capacity

Recommendation: Adopt a clear definition of capacity for minors.

Rationale: The act uses a standard of capacity to determine whether a minor can exercise certain rights and powers with respect to their data. Given the stark differences between "capable" minors and ones who are not, a definition of capacity is key. One example is from Ontario's *Personal Health Information Protection Act*, where capacity denotes an ability "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."[15] However, minors should not be disempowered because of their difficulty in understanding complex information processing environments. Adults, too, often fail to understand the nature and consequences of big data processing techniques. Capacity should thus focus more on the broader picture of a given scenario, like how patients are not required to understand the nuances of a proposed medical procedure.

5. Use an age-based threshold complemented with capacity

Recommendation: Set 13 as the age at which a minor can exercise a right or a power under the CPPA and then use capacity to complement the age-based rule. For example, a "capable" (i.e.., possessive of capacity) 12 year-old should also be allowed to exercise a right or power under the CPPA without their legally authorized representative.

---

[13] Article 17, *International Covenant on Civil and Political Rights*, United Nations Treaty Series, vol. 999, p. 171, 1966.

[14] Article 16, *Convention on the Rights of the Child*, United Nations Treaty Series, vol. 1577, p. 3, 1989.

[15] Section 21, *Personal Health Information Protection Act, 2004*, SO 2004, c 3, Schedule A.

Rationale: In its current state, the CPPA allows a willing, capable minor to exercise their rights and powers ("recourses") without their legally authorized representative (s. 4). However, capacity alone is not a workable concept for most organizations collecting, using, or disclosing a minor's personal information; most will have had limited or no direct contact with the minor concerned. Capacity would be difficult to ascertain in these circumstances. By setting the age at which minors can exercise a right or power under the CPPA at 13, the CPPA would have continuity with the Office of the Privacy Commissioner's existing consent guidelines while nevertheless raising the bar for protections of minors' personal information through its other provisions.[16]

Nevertheless, capacity can be useful for minors with maturity beyond their years. We thus recommend using capacity as a complement to the age-based thresholds to allow mature minors under the age of 13 to exercise rights and powers under the act. This would dovetail with the concept of "evolving capacities" under the *Convention on the Rights of the Child.*[17]

6. Clarify the relationship between a minor's capacity/age and parental decision-making

Recommendation: The CPPA should make explicit that in cases of differing opinions about the exercise of rights and recourses under the Act between capable minors and their legally authorized representatives (e.g., parents, guardians, tutors), the wishes of the capable minor are to prevail.

Rationale: Including this provision avoids a potential stalemate between a competent minor and their legally authorized representative. Some provincial data protection laws have similar provisions.[18]

7. Specify rules for age and parental consent verification

Recommendation: Consider specifying rules for age and parental consent verification. These rules should include a risk-based, proportionate approach to verification methods (see rationale, below), a recognition of the importance of freedom of expression, an absolute purpose limitation that any information collected, used, or disclosed for verification purposes will not be used for anything other than those same verification purposes, and an obligation to store this collected information for the shortest possible time period. Both minors and their legally authorized representatives should be consulted.

Rationale: Creating differentiated rules between minors and adults with an accompanying reliance on parental consent in certain cases implies a need for methods of age (or capacity) and parental consent verification. Such verification can be as intrusive as requiring government-issued photo identification to be submitted, giving rise to further data protection and cybersecurity concerns. Beyond data protection issues, these verification procedures can have wide-reaching effects on freedom of expression online. By adopting a risk-based approach, instances of collection, use, or disclosure of personal information that pose a lower risk to a minor would be subject to less onerous verification procedures for either age or parental consent.

---

[16] Office of the Privacy Commissioner of Canada, "Guidelines for obtaining meaningful consent", (13 August 2021), online: <https://www.priv.gc.ca/en/privacy-topics/collecting-personal-information/consent/gl_omc_201805/>.

[17] Lansdown, Gerison. "The Evolving Capacities of the Child." Florence: UNICEF Office of Research - Innocenti, 2005.

[18] Section 23(3), *Personal Health Information Protection Act, 2004*, SO 2004, c 3, Schedule A.

8. Clarify the rights of individuals regarding data collected when they were a minor and/or on the basis of parental consent

Recommendation: Better specify what happens when a minor reaches the age of majority. In particular, specify that (1) information about a minor includes information collected, used, or disclosed at any time when an individual was a minor and that (2) entities must seek the consent of the former minor within a specified time of them reaching the age of majority where parental consent was previously relied upon.

Rationale: The sensitivity of information generated during one's childhood does not necessarily disappear upon attaining the age of majority. Indeed, personal information from one's childhood may often become more sensitive because it does not cohere with one's identities as an adult. The plasticity and development of identities in childhood (and throughout adulthood) should be supported and this includes, for example, a robust right of deletion for personal information about one's childhood.

If an organization is relying upon the consent given by parents to legitimate the ongoing collection, use, disclosure, or retention of personal information, re-consenting via either an opt-in or opt-out model at the age of majority should be mandated. (This approach is already done for health research in Canada.[19]) Doing so would allow young adults to decide whether they would like their personal information to continue to be processed by organizations and gives the potential for a "blank slate" upon reaching the age of majority. We also note that the pervasiveness of data collection in children's lives today makes it unfeasible to expect individuals to maintain a list of every entity who has their data, whereas entities can easily contact children around the time at which they are no longer minors.

9. Oblige the Commissioner to develop guidelines for children's information with robust participation from children

Recommendation: The Office of the Privacy Commissioner should be given an express mandate for creating clear guidelines regarding children's personal information. These guidelines should be developed in conjunction with youth and grounded in empirical research about children's understandings and experiences with privacy.[20] Furthermore, the guidelines should be based in existing general principles about children's privacy and will serve organizations by making the process of collecting, using, or disclosing children's personal information more straightforward while maintaining robust guarantees for children.

Rationale: The CPPA's provisions for children's personal information remain at a high level of generality. Issues concerning plain language requirements (s. 15(4)), consent (s. 15), appropriate purposes (s. 12), retention policies (s. 53(2)), security safeguards (s. 57(1)), and breach notifications (s. 58(8)(a)) all have child-specific dimensions. Organizations will benefit from clarity regarding what these general concerns require of them when they are applied to children's personal information. We note the importance of the existing guidelines from the Office of the Privacy Commissioner in doing this under *PIPEDA*. These

[19] Murdoch, Blake, Allison Jandura & Timothy Caulfield, "Reconsenting paediatric research participants for use of identifying data" (2022) Journal of Medical Ethics, online: <https://jme.bmj.com/content/early/2022/01/18/medethics-2021-107958>.

[20] See, e.g., Third, Amanda & Lilly Moody, *Our rights in the digital world: A report on the children's consultations to inform UNCRC General Comment 25* (London and Sydney: 5Rights Foundation and Western Sydney University, 2021).

guidelines have not, however, been developed through consultation with youth.[21] Taking it as an unfortunate foregone conclusion that youth will not be consulted for this bill, requiring youth engagement for the development of guidelines is a second best. Doing so gives effect to the child's right to be heard under the *Convention on the Rights of the Child*. The UN Committee on the Rights of the Child's *General comment No. 25 (2021) on children's rights in relation to the digital environment* was undertaken with extensive consultation with youth around the world – including Canadian youth.[22] Under this model, children's privacy can be governed in accordance with international principles regarding the rights of the child and provide clarity for Canadian businesses and organizations.

10. Oblige the Commissioner to develop a children's design code with robust participation from children

Recommendation: The Office of the Privacy Commissioner should be mandated to develop a children's design code.

Rationale: Design codes are age-appropriate data protection safeguards that companies must build into services that children are most likely to access in order to provide the highest level of privacy by design, including in default settings (e.g., location sharing, auto-recommenders, notifications and nudges).[23] The draft CPPA currently gives the OPC the power to develop a design code (s. 110(1)(b)), but it is not under a statutory duty to do so. (We note that in the United Kingdom, the Information Commissioner's Office had a statutory duty to develop a children's code.[24])

Design codes guide the design and implementation of youth-targeting services that use personal information. Design codes respond to the fact that the circumstances in which youth disclose information are heavily influenced by the design of the service. A design code manages issues such as dark patterns, which undermine user autonomy. Prevalent in children's digital games and apps, dark patterns "describe design practices that trick or manipulate users into making choices they would not otherwise have made and that may cause harm".[25]

---

[21] Although youth engagement is already a priority with the Office of the Privacy Commissioner. See Goss Gilroy Inc for the Office of the Privacy Commissioner of Canada, "Evaluation of Work Under the Strategic Privacy Priorities: Consent Model & Youth Initiatives", (8 March 2022), online: <https://www.priv.gc.ca/en/about-the-opc/opc-operational-reports/audits-and-evaluations-of-the-opc/internal-opc-audits-and-evaluations/2021/iac_youth_2021/>.

[22] Third, Amanda & Lilly Moody, *Our rights in the digital world: A report on the children's consultations to inform UNCRC General Comment 25* (London and Sydney: 5Rights Foundation and Western Sydney University, 2021).

[23] Information Commissioner's Office (UK), "Introduction to the Children's code", (1 September 2023), online: <https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/childrens-information/childrens-code-guidance-and-resources/introduction-to-the-childrens-code/>.

[24] Section 123, *Data Protection Act*, c 12 2018.

[25] *Bringing Dark Patterns to Light* (Washington, DC: Federal Trade Commission Bureau of Consumer Protection, 2022).

Beyond children's right to privacy, the design of digital environments implicates children's rights to play, culture, and protection from economic exploitation under the *Convention on the Rights of the Child*.[26] A properly developed design code can accordingly help secure a broad array of children's rights. To succeed, design codes should be grounded in how young people use online platforms. For example, they should enable youth to play with different online identities and engage in nuanced disclosure practices with their peers and social groups.[27]

[26] *General comment No. 25 (2021) on children's rights in relation to the digital environment* (United Nations Committee on the Rights of the Child, 2021) CRC/C/GC/25; Hof, Simone van der et al, "The Child's Right to Protection against Economic Exploitation in the Digital World" (2020) 28:4 The International Journal of Children's Rights 833–859.

[27] Steeves, Valerie, "Privacy, sociality and the failure of regulation: lessons learned from young Canadians' online experiences" in Beate Roessler & Dorota Mokrosinska, eds, *Social Dimensions of Privacy: Interdisciplinary Perspectives* (Cambridge, UK: Cambridge University Press, 2015) 244.