Every Child Left Behind: How Bill C-27 Fails to Adequately Protect the Privacy Rights of Canada's Children

George Hua and Vivek Krishnamurthy

June 2023

cippic Samuelson-Glushko **Canadian Internet Policy and Public Interest Clinic**
Clinique d'Intérêt publique et de politique d'Internet du Canada Samuelson-Glushko

uOttawa

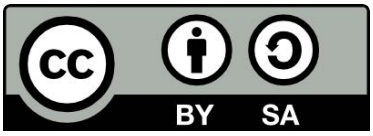
About CIPPIC

CIPPIC is Canada's first and only public interest technology law clinic. Based at the Centre for Law, Technology and Society at the University of Ottawa's Faculty of Law, our team of legal experts and law students works together to advance the public interest on critical law and technology issues including privacy, free expression, intellectual property, telecommunications policy, and data and algorithmic governance. For more information, visit our website at www.cippic.ca.

About the Authors

George Hua is a CIPPIC student intern and a third-year law student in the English common law program at the University of Ottawa's Faculty of Law.

Vivek Krishnamurthy is the Director of CIPPIC and the Samuelson-Glushko Professor of Law at the University of Ottawa's Faculty of Law.



The layout of this report was conceived by Yuan Stevens. Matthew Tai, Gareth Spanglett, and Julia Kafato provided editorial assistance. Cover image art by Vidmir Raic from Pixabay.com.

Table of Contents

Summary

Children deserve strong privacy protections in a data-driven economy. As children spend ever-increasing amounts of time online and corporations collect and commercialize their data, stronger privacy protections for children are necessary. Canada's proposed Bill C-27 aims to overhaul and strengthen Canada's weak and outdated laws protecting online privacy, but unfortunately the bill falls short when protecting children's privacy interests in Canada.

This report compares the children's privacy protection provisions in the *Consumer Privacy Protection Act* (CPPA)—a key component of Bill C-27—with the United Kingdom's Age-Appropriate Design Code and California's *Age-Appropriate Design Code Act*. It finds that Bill C-27 falls short compared to these laws and represents a missed opportunity to address this important issue of children's privacy in the digital age.

This report also recommends the inclusion of certain key features into the *CPPA* to enhance the objective of children's privacy protection, namely, to include "best interest of the child" language; a default setting requirement; and a data protection impact assessment framework. Finally, the report addresses potential constitutional objections to the federal government enacting stronger children's privacy protections for children by citing to past examples of analogous child safety measures.

Introduction

Children's privacy is a pressing issue in modern-day society as technology becomes more integrated in the lives of children. Children now have more access than ever to devices such as smartphones, tablets, smart toys, and AI assistants. All these devices collect an abundance of data using microphones, cameras, and other integrated sensors to serve the manufacturer's commercial purpose.[1] The COVID-19 pandemic has further entrenched children's use of online technology through trends such as online schooling and gaming.

Canada has long lacked adequate laws to protect children's privacy. Unlike even the U.S., which has a federal statute dedicated to this issue,[2] Canada has no specific laws in place to protect children's privacy. On June 16th, 2022, the Canadian government introduced Bill C-27: *Digital Charter Implementation Act, 2022*.[3] The primary purpose of Bill C-27 is to reform the *Personal Information Protection and Electronic Documents Act* (*PIPEDA*). The *Consumer Privacy Protection Act* (*CPPA*) under Bill C-27 will repeal and replace the existing Canadian privacy regulatory framework in the now 20-year-old PIPEDA.

Many critics have expressed discontent towards the Government of Canada's lackluster effort to reform Canada's privacy protection regime.[4] Prominent information law scholars such as Teresa Scassa have highlighted issues within Bill C-27 regarding the definition of de-identification, the new exception to allow organizations to collect or use personal data without knowledge or consent, among others.[5] This report builds on existing critiques of Bill C-27 to explain how the legislation fails Canada's children, and falls short of measures introduced in peer jurisdictions (notably California and the United Kingdom) when it comes to protecting the privacy rights of our most vulnerable citizens.[6]

---

[1] Alexandre Plourde, "Monitoring children: privacy in the world of smart toys" (2018), online: *Office of the Privacy Commissioner of Canada* <www.priv.gc.ca/en/opc-actions-and-decisions/research/funding-for-privacy-research-and-knowledge-translation/completed-contributions-program-projects/2017-2018/p_201718_01>.

[2] *Children's Online Privacy Protection Act of 1998*, 15 USC § 6501 (2018).

[3] 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*, 1st Sess, 44th Parl, 2022 (first reading 16 June 2022) [Bill C-27].

[4] Michelle Gordon, "Children's right to privacy needs to be strengthened in law and beyond", *Policy Options* (12 January 2023), online: <policyoptions.irpp.org/magazines/january-2023/tech-child-privacy-laws>; Ken Rubin, "Canadians' privacy could take a serious hit this coming legislative session", *The Hill Times* (16 January 2023), online: <www.hilltimes.com/story/2023/01/16/canadians-privacy-could-take-a-serious-hit-this-coming-legislative-session/360839>; Michael J.S. Beauvais & Leslie Regan Shade, "How will Bill C-27 impact youth privacy?" (8 November 2022), online: *University of Toronto* <srinstitute.utoronto.ca/news/how-will-bill-c-27-impact-youth-privacy>; Michael Geist, "The Groundhog Day Privacy Bill: The Government Waited Months to Bring Back Roughly the Same Privacy Plan?!" (17 June 2022), online (blog): *Michael Geist* <www.michaelgeist.ca/2022/06/the-groundhog-day-privacy-bill>.

[5] Teresa Scassa, "Anonymization and De-identification in Bill C-27" (6 July 2022), online (blog): *Teresa Scassa* <www.teresascassa.ca/index.php?option=com_k2&view=item&id=356:anonymization-and-de-identification-in-bill-c-27&Itemid=80>; Teresa Scassa, "Bill C-27's Take on Consent: A Mixed Review" (4 July 2022), online (blog): *Teresa Scassa* <www.teresascassa.ca/index.php?option=com_k2&view=item&id=355:bill-c-27%E2%80%99s-take-on-consent-a-mixed-review&Itemid=80>.

[6] Teresa Scassa, "Bill C-27 and Children's Privacy" (25 July 2022), online (blog): *Teresa Scassa* <www.teresascassa.ca/index.php?option=com_k2&view=item&id=360:bill-c-27-and-children%E2%80%99s-privacy&Itemid=80> [Scassa].

Our report benchmarks the *CPPA's* child-centric measures against similar measures in the UK and California[7] and identifies three key features that should be added to the *CPPA*: (1) "best interest of the child" language; (2) a privacy-protective default setting requirement for children; and (3) data protection impact assessment requirements when children's privacy interests are at stake.

This report is divided into four parts:

Part 1 describes the new children's privacy protection provisions in the *CPPA*.

Part 2 compares the children's privacy protection provision in the *CPPA* with similar legislation in the UK and California and provides recommendations for the *CPPA*.

Part 3 addresses the constitutionality of defining a federal age of majority in the *CPPA* for the purpose of public safety.

Part 4 summarizes our conclusions and recommendations.

1. Children's Privacy Protection in the *CPPA*

Bill C-27 and the *CPPA* expand upon the previous *PIPEDA* reform bill (C-11) and includes several provisions for protecting children's privacy.

The most important addition in the *CPPA* is found in section 2(2), which deems "the personal information of minors" as "sensitive information."[8] The Office of the Privacy Commissioner of Canada (OPC) has defined sensitive information to be certain types of personal information that contain specific risks to individuals and require a higher degree of protection.[9] Examples of sensitive information include health and financial data, ethnic and racial origins, political opinions, and genetic and biometric data. By designating a minor's information as "sensitive," entities handling this type of data will be held to a more rigorous set of standards under the new legislation. This includes taking extra precautions in areas such as data retention policies, developing security safeguards for personal information, reporting data breaches, measures taken for data de-identification, and the development of privacy management programs.[10] However, the *CPPA* fails to define the term "minor" in the Act, and the term is defined differently in federal, provincial, and territorial legislation.

Other *CPPA* provisions relating to children's privacy include section 4(a), authorized representatives, and section 55(2), the right of erasure.[11] Section 4(a) of the *CPPA* allows a parent, guardian, or tutor to exercise rights and recourses under the *CPPA* on behalf of a minor, including the right to consent.

---

[7] UK, Information Commissioner's Office, *Age appropriate design: a code of practice for online services*, (Wilmslow: ICO, 2019) [UK Code]; US, AB 2273, *An act to add Title 1.81.47 (commencing with Section 1798.9928) to Part 4 of Division 3 of, and to repeal Section 1798.99.32 of, the Civil Code, relating to consumer privacy*, 2021-2022, Reg Sess, Cal, 2022 [California Act].

[8] Bill C-27, *supra* note 3, s 2(2).

[9] Canada, Office of the Privacy Commissioner of Canada, *Interpretation Bulletin: Sensitive Information* (Ottawa: OPC, 2022), online <www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/pipeda-compliance-help/pipeda-interpretation-bulletins/interpretations_10_sensible>.

[10] Bill C-27, *supra* note 3, ss 9(2), 53(2), 57(1), 58(5), 62(2)(e) & 109.

[11] *Ibid*, s 4 & 55.

However, minors may also choose to personally exercise their rights if they wish and are capable of doing so.[12] The *CPPA* fails to provide any guidance on how to evaluate capacity, however. If a parent and a minor disagree with respect to providing consent for an online service, the business associated with the online service may be placed in the uncomfortable position of having to determine whether the minor has the capacity to provide consent.

Section 55 allows individuals to submit written requests to an organization to dispose of their personal information.[13] Section 55(2)(d) affirms a minor's right to erasure by explicitly providing that an organization cannot deny the request by a minor to delete their personal information on the basis of information retention policies. There are several exceptions specified under section 55(2), however section 55(2)(d) and (f) stipulate that these exceptions do not apply to the personal information of minors.[14]

2. The CPPA's Children's Privacy Protections in International Context

There have been significant developments in peer jurisdictions in terms of protecting privacy of children, notably in the UK and California. In the UK, the *Age-Appropriate Design Code* came into effect in 2020. The UK Code sets out 15 design standards that companies must implement when developing products or services that are "likely to be accessed by children."[15] The scope of the UK Code is wide and it adopts the UN's definition of "child," which is defined as anyone "below the age of 18."[16] On September 15th, 2022, California enacted its *Age-Appropriate Design Code Act*, which will come into force on July 1st, 2024.[17] The California Act is modeled after the UK Code and contains many similar features for regulating online platforms to proactively protect children's privacy in their design and operation.

CIPPIC believes that several key features of the UK and California's legislation should be added to the new *CPPA* to strengthen and improve the objective of enhancing children's privacy in Canada.

Recommendation #1: "Best interest of the child" language

We recommend incorporating the "best interest of the child" language into the *CPPA*. This would require companies developing or providing online services and products for children to take the "best interest of the child" into account as the primary consideration in all design decisions implicating the rights of children. Both the UK Code and the California Act expressly state that the best interest of the child must be considered when designing or developing online services and products for children.[18] The California Act further states that if there is a conflict between commercial interests and the best interest of the child, companies "should prioritize the privacy,

---

[12] *Ibid*, s 4.
[13] *Ibid*, s 55.
[14] *Ibid*, s 55(2).
[15] UK Code, *supra* note 7 at 5.
[16] *Convention on the Rights of the Child*, 20 November 1989, UNTS 1577 at 3 (entered into force 2 September 1990) [UNCRC].
[17] California Act, *supra* note 7.
[18] UK Code, *supra* note 7 at 24; California Act, *supra* note 7 at 1798.9929(a).

safety, and well-being" of the child.[19] The UK also created the Best Interest Framework to help guide companies by clarifying and emphasizing the rights most likely to be impacted by data collection and processing.[20] Introducing the "best interests of the child" concept into the *CPPA* is consistent with Canada's legal obligations under Article 3 of the *UN Convention of the Rights of the Child* (UNCRC). Canada signed and ratified the UNCRC in 1991. The Article states that "[i]n all actions concerning children … the best interests of the child shall be a primary concern."[21]

Recommendation #2: Privacy-Protective Default Settings

Both the UK Code and the California Act require online services and products that are likely to be accessed by children to set their privacy settings to "high" by default. Any company that, by default, offers a different setting must demonstrate that the different privacy setting is in the "best interests" of children.[22]

We believe that the CPPA should incorporate such requirements, too. Companies that develop products or services that are likely to be accessed by children should be required to automatically set their privacy settings to the highest level. This would include automatically turning off geo-location tracking and prohibiting optional uses of personal data obtained through the online service or product, including any uses to personalize the user experience of the service or product. This requirement aligns with section 2(2) of the *CPPA*, which designates personal information of minors as "sensitive" information.[23]

Requiring the default privacy settings for children to be set on high is consistent with the OPC's findings in the Nexopia matter.[24] Nexopia, the largest youth-oriented social networking website at the time, set the privacy setting for all of its users to "visible to all." Correspondingly, user profiles could be searched via external search engines to gather personal information on Nexopia users, The OPC investigated and recommended Nexopia change its default privacy setting. The OPC stated that while establishing default privacy settings may be appropriate, the users must be properly informed of the implications of the different settings and the pre-selected settings must be reasonable.[25]

Recommendation #3: Data Protection Impact Assessments (DPIA)

Lastly, we recommend that the *CPPA* should mandate DPIAs when dealing with children's data. A DPIA is a defined process that helps companies identify and minimize data protection risk of their service or product.[26] With a DPIA, the company must consider the risk to individuals' rights and freedoms of individuals and assess the likelihood and the severity of any impacts. DPIAs are a centerpiece of the European Union's General Data Protection Regulation (*GDPR*)—the world's most

---

[19] California Act*, supra* note 7 at 1798.9929(a).
[20] UK, Information Commissioner's Office, *Children's Code: Best Interests Framework*, (Wilmslow: ICO, 2021).
[21] UNCRC, *supra* note 16 at 45.
[22] California Act*, supra* note 7 at 1798.99.31(a)(6).
[23] Bill C-27, *supra* note 3.
[24] Canada, Office of the Privacy Commissioner of Canada, *Social networking site for youth, Nexopia, breached Canadian privacy law* (Ottawa, OPCC, 2012) [Nexopia].
[25] *Ibid* at para 92.
[26] UK, Information Commissioner's Office, *Guide to the General Data Protection Regulation (GDPR)* (2022) at 201.

comprehensive data privacy law—and the concept of requiring DPIAs is a feature of an increasing number of privacy laws around the world.[27]

The UK Code requires companies to complete a DPIA before the commencement of any new online service or product, or when there are plans to make significant changes to an existing service or product that is likely to be accessed by children.[28] The DPIA must state the nature, scope, context, and purpose of the information collection, and larger organizations are expected to conduct consultations from the public to solicit opinions. The DPIA must also be conducted for *any* type of data collection or use that is likely to result in a high risk to the rights and freedoms of individuals.[29] The California Act follows the same line of logic, but with a specific emphasis on harm to children.[30]

The CPPA has a similar assessment mechanism, but it only applies to exceptions to consent, which creates a structural weakness in the *CPPA* that needs to be addressed. Section 18(4) of the *CPPA* requires that prior to the collection or the usage of personal information, organizations must identify any potential adverse effects on the individual, take reasonable measures to reduce or mitigate the adverse effect, and comply with any prescribed requirement.[31]

The limited DPIA provision does not apply to minors at all. Minors' information is deemed to be "sensitive information" pursuant to section 2(2) of the *CPPA*, and therefore requires express consent for its collection. The DPIA provision only applies to implied consent scenarios where companies can collect or use information without individual's consent or knowledge. Minors' information falls outside of this category, and thereby bypasses the DPIA provision in the *CPPA*. Section 18(4) should be moved to another section of the *CPPA* so that it is not only applicable to implied consent circumstances.

3. Protecting Children's Privacy in Canada: Federalism Considerations

Leading scholars have suggested that the *CPPA* is modest in its attempt to address children's privacy because the federal government is concerned with constitutional issues relating to the division of powers when it comes to regulating children's online privacy.[32] Such fears may be overstated, given that the federal government has long used its trade and commerce power under s. 91(2) of the *Constitution Act, 1867* to protect children from dangerous products. The same constitutional provisions that support federal action to protect children against dangerous physical products can also be relied upon to protect children from digital products and services that endanger their privacy.

Consider, for example, the many regulations enacted by the federal government under the *Canada Consumer Product Safety Act* that impose additional requirements on companies that provide

---

[27] Margot E Kaminski & Gianclaudio Malgieri, "Algorithmic impact assessments under the GDPR: producing multi-layered explanations" (2020) 11:2 Intl Data Privacy L 125.
[28] UK Code, *supra* note 7 at 27.
[29] EU, *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016*, [2016] OJ 119/1 at 53.
[30] California Act, *supra* note 7 at 1798.99.30(b)(2).
[31] Bill C-27, *supra* note 3, s 18(4).
[32] Scassa, *supra* note 6.

products or services to children—from toys to sleepware.[33] MPs and Senators have also repeatedly emphasized the importance of protecting children's safety and health, and how products geared towards children warrant special attention when it comes to product safety concerns.[34] Likewise, the safety of children when using digital products and services merits the same federal attention and regulation as what has been afforded to tangible physical products. Indeed, one can argue that the CPPA is a species of product safety legislation that protects Canadians from digital products and services that pose a danger to their privacy. If Parliament is entitled to enact product safety legislation under the federal trade and commerce powers for tangible, physical products, it should be able to do so in an online context as well.

Furthermore, it is not unprecedent for the federal government to specify who is a "minor" in legislation regulating the market for licit goods. In Canada, the age of majority is determined by each province and territory according to section 92(13) of the *Constitution Act*.[35] This has not prevented the federal government from imposing age limits to protect children's health and safety, however.

Consider, for example, the *Tobacco and Vaping Products Act*, which restricts the sale or delivery of tobacco or vaping products to young people, and prohibits the promotion of a vaping product in a manner that could be seen as appealing to young persons.[36] This legislation defines a "young person" as a person under 18 years of age.[37] Similar provisions can also be found in the *Cannabis Act*, where the distribution, possession, and promotion to a "young person" is strictly prohibited.[38]

There are many instances where both a federal and a provincial age limit operate in parallel in the interest of public safety and children's safety. A federally imposed age limit would establish a national minimum, while the provinces and territories may set a higher minimum age limits should they wish to do so.[39] For example, in the case of alcohol and tobacco sales, the federal government set the legal age for purchase at 18, while many provinces determined that a higher bar was required and set the age limit at 19.[40] The same could be true with regard to children's privacy, to the extent that provincial governments enact laws that are "substantially similar" to the *CPPA* and incorporate stronger privacy protections for children.[41]

Therefore, the federal government should define the term "minor" in the *CPPA* to clarify who exactly benefits from the enhanced privacy protections that the bill should provide to young people.

---

[33] *Canada Consumer Product Safety Act*, SC 2010, c 21 [*CCPSA*]; *Children's Jewellery Regulations*, SOR/2018-82; *Children's Sleepware Regulations*, SOR/2016-169; *Toys Regulations*, SOR/2011-17.

[34] "Bill C-36, An Act respecting the safety of consumer products", 3rd reading, *Debates of the Senate*, 40-3, No 147 (9 December 2010) at 1568 (Hon Joseph a Day); House of Commons, Standing Committee on Health, *Evidence*, 40-3, No 32 at 1105 & 1145 (Hon Leona Aglukkaq).

[35] *Constitution Act, 1982*, s 92(13) [*Constitution Act*].

[36] *Tobacco and Vaping Products Act*, SC 1997, c 13, ss 8(1), 9(1) & 30.1 [*Tobacco Act*].

[37] *Ibid*, s 2.

[38] *Cannabis Act*, SC 2018, c 16, ss 8(1), 9(1), 17(1) & 32(1).

[39] Canada, Task Force on Cannabis Legalization and Regulation, *A Framework for the Legalization and Regulation of Cannabis in Canada: The Final Report of the Task Force on Cannabis Legalization and Regulation* (Ottawa: Health Canada, 2016) at 16.

[40] *Ibid*.

[41] Office of the Privacy Commissioner of Canada, "Provincial laws that may apply instead of PIPEDA" (May 2020), online: *OPC* <www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/r_o_p/prov-pipeda>.

Defining the term “minor” would provide the necessary clarity in the regulatory framework for companies to comply. There are no serious constitutional barriers to the federal government doing so, as evidenced by the government's previous use of age limits to protect children's health and safety.

4. Conclusion

The *CPPA* risks becoming outdated upon enactment because it falls short compared to other children’s privacy protection laws globally. The legislation merely does the bare minimum to protect children’s privacy rights, as evidenced by the limited use of the term “minor” throughout the bill.

Children’s privacy is an important objective in the modern world. Children spend a great deal of time online, and the wide availability of electronic toys and devices only propagate the associated privacy risks for children. Bill C-27 provides a great opportunity to build certain legal principles and concepts promoting privacy protection for children and empower the Privacy Commissioner to provide further guidance in this area in the future.