A Critical Look at Bill C-27's *Consumer Privacy Protection Act*

January 2024

Michelle Hennessey and Shaarini Ravitharan

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

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.

Table of Contents

Executive Summary

Technology is evolving quickly, and Canadians urgently need a privacy regime that provides meaningful protection in the modern digital environment. As commercial pressure to collect and share personal information intensifies, the modernization of Canada's privacy regime should prioritize strong protections that allow Canadians to exercise autonomous choice over their personal information. The need for real and effective privacy protection is especially acute for sensitive information such as health data, and for vulnerable populations such as children. Canadians require safeguards that ensure meaningful consent, particularly in a marketplace increasingly shaped by data brokers and the widespread use of dark patterns.

Robust privacy laws are not at odds with innovation; the relationship between the two is interdependent and must be acknowledged. In the digital age, privacy law is not only about safeguarding individuals' human rights, but about safeguarding those rights in a way that cultivates responsible and ethical innovation. Doing so promotes Canadians' trust in new technologies and, in turn, fosters further innovation and responsible market development.

Part 1 of Bill C-27, the *Digital Charter Implementation Act, 2022*, would enact the *Consumer Privacy Protection Act* (CPPA), a comprehensive overhaul of Canada's outdated private sector privacy laws. Although the CPPA represents a welcome and necessary modernization, it falls short in several respects. To address these shortcomings, CIPPIC offers six recommendations to strengthen the CPPA and safeguard the fundamental human right to privacy, each inspired by and harmonized with leading international standards.

Summary of CIPPIC's recommendations:

1. **Recognize personal information protection as a fundamental human right.**
2. **Strengthen and refine the CPPA's scope.**
   - 2.1. Define "sensitive information."
   - 2.2. Include a data protection impact assessment framework.
   - 2.3. Keep anonymized data within scope of the CPPA.
   - 2.4. Bring federal political parties under the CPPA.
3. **Put individuals at the centre of consent and its exceptions.**
   - 3.1. Ensure consent remains meaningful.
   - 3.2. Remove the ability to imply consent.
   - 3.3. Make exceptions to consent easy for individuals to understand.
   - 3.4. Prioritize fundamental rights over business interests.
   - 3.5. Increase transparency and accountability in cases of exceptions to consent.
4. **Strengthen protections for children's privacy.**
   - 4.1. Include "best interest of the child" language.
   - 4.2. Ensure children's privacy is considered during data protection impact assessments.
   - 4.3. Require privacy settings be set to "high" by default.
   - 4.4. Provide framework to determine a minor's capacity to consent.
5. **Dark Patterns**
   - 5.1. Define "dark patterns."
   - 5.2. Recognize that consent obtained through dark patterns is void.
6. **Create a framework for managing data brokers.**
   - 6.1. Define "data brokers."
   - 6.2. Recognize a fiduciary duty owed by data brokers.
   - 6.3. Require data brokers to adhere to increased transparency requirement.

Introduction

On June 16, 2022, the Canadian government introduced Bill C-27: *Digital Charter Implementation Act, 2022*.[1] Part I of Bill C-27, the *Consumer Privacy Protection Act* (CPPA), will repeal and replace the existing 20-year-old private-sector privacy framework under the *Personal Information Protection and Electronic Documents Act* (PIPEDA).[2] The CPPA aims to "build a stronger framework for privacy protection" and to introduce reforms that better align Canadian privacy legislation with international best practices, including the European Union's (EU) *General Data Protection Regulation* (GDPR).[3]

Building on prior critiques of the CPPA, this submission recommends amendments that would better achieve the government's intended purpose. While the CPPA improves on PIPEDA in many respects, it falls short by:

- failing to recognize privacy as a fundamental human right;
- scoping anonymized data outside the CPPA;
- failing to bring political parties under the CPPA;
- restructuring exceptions to consent to prioritize commercial interests over individual rights;
- providing inadequate protection for children; and
- ignoring the prevalence of data brokers and dark patterns.

CIPPIC's recommendations would meaningfully protect individuals' privacy rights, including children, and align Canada with leading international frameworks for privacy and responsible innovation: the EU's GDPR, the United Kingdom's *Data Protection Act 2018* and *Age-Appropriate Design Code* (UK Code), and California's *Age-Appropriate Design Code Act* (California Design Code).[4]

---

[1] 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 (second reading 24 April 2023).

[2] 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, Part I (second reading 24 April 2023) [CPPA]; *Personal Information Protection and Electronic Documents Act*, SC 2000, c 5 [PIPEDA].

[3] As explained by the Honourable Minister Champagne; House of Commons, Standing Committee on Industry and Technology, *Evidence*, 44-1, No 86 (26 September 2023) at 1631 (Hon François-Philippe Champagne); Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), [2016] OJ, L 119/1 [GDPR].

[4] *Data Protection Act 2018* (UK), 2018, c 12 [Data Protection Act]; *Age appropriate design: a code of practice for online services* [UK Code], Information Commissioner's Office (UK), 2020; *The California Age-Appropriate Design Code Act*, CA Civ Code § 1798.99.28–1798.99.40 (2023) [California Design Code]. The *California Age-Appropriate Design Code Act* was preliminarily partially enjoined in *NetChoice, LLC v. Bonta*, 152 F.4th 1002 (9th Cir. 2026), on First Amendment grounds. This submission relies on the Act as an influential legislative model rather than as settled constitutional law.

Canada faces a rare opportunity to modernize its privacy regime and must act decisively. Canadians deserve legislation that recognizes privacy as a right of heightened significance in the digital age and defends it with strong legal protections.

Sustainable innovation and economic growth require privacy

CIPPIC's recommendations would ensure the CPPA delivers meaningful protection for Canadians' privacy rights while promoting innovation. Lawmakers must understand the CPPA as a keystone of long-term economic growth: the commercial appeal of digital innovation depends on public trust in how new technologies handle personal data.[5] To secure that trust, the CPPA must promote responsible innovation grounded in Canadians' right to privacy.

Distrust poses a direct threat to sustainable economic growth in the digital market.[6] Privacy is the most widely discussed concern about new communication technologies, a concern made acute by the concentration of market power among organizations whose profits rest on the constant surveillance of consumers and exploitation of their data.[7] Over half of Canadians report no trust in how social media companies use personal data, and more than a quarter report the same about "big tech" companies (55% and 27% respectively).[8] More than half also doubt that organizations respect their privacy rights, a figure that fell six percentage points between 2020 and 2022 alone (from 45% to 39%).[9] Lawmakers should treat these numbers as a serious warning: Canadians' distrust of the privacy practices of large digital innovators signals a market failure and a crisis of confidence that could generate market volatility.[10]

Privacy legislation must promote responsible innovation to build the trust that underpins stable long-term growth in the digital market.[11] Innovation legislation must therefore draw on societal and ethical norms, including privacy, while privacy legislation must require organizations to build substantive privacy protections into the design of new products and services ("privacy by design").[12] Effective privacy legislation must also be legible to Canadians, advance transparency and dialogue between Canadians and the organizations that handle their personal information, and confront business models that erode trust by exploiting personal data.

---

[5] Office of the Privacy Commissioner of Canada, "Submission of the Office of the Privacy Commissioner of Canada on Bill C-11, the Digital Charter Implementation Act, 2020" (11 May 2021) [OPC, "Submission on Bill C-11"].

[6] *Ibid*.

[7] Bernd Carsten Stahl and Emad Yaghmaei, "The Role of Privacy in the Framework for Responsible Research and Innovation in ICT for Health, Demographic Change and Ageing" in Anja Lehmann et al., eds, *Privacy and Identity Management* (Cham: Springer International Publishing, 2016) 92 at 96; House of Commons, Standing Committee on Industry and Technology, *Evidence*, 44-1, No 107 (31 January 2024) at 1755 (Vass Bednar).

[8] Office of the Privacy Commissioner of Canada, "2022-23 Survey of Canadians on Privacy-Related Issues" (January 2023).

[9] *Ibid*.

[10] See Nicholas Economides and Ioannis Lianos, "Restrictions On Privacy and Exploitation In The Digital Economy: A Market Failure Perspective" (2021) 17:4 J of Competition L & Economics 765.

[11] OPC, "Submission on Bill C-11", *supra* note 5.

[12] Daniele Ruggiu *et al*, "Responsible Innovation at Work: Gamification, Public Engagement, and Privacy by Design" (2022) 9:3 J Responsible Innovation 315 at 324.

1. Recognize personal information protection as a fundamental human right

Privacy is an internationally recognized human right, and Canadian legislation must acknowledge that status and accord privacy commensurate legal weight. CIPPIC joins the many voices calling upon the government to recognize privacy as a fundamental human right in the text of the CPPA itself.[13]

The Office of the Privacy Commissioner recommends including language that qualifies privacy as a "fundamental right" in the preamble and section 5 of Bill C-27.[14] Minister Champagne has proposed similar amendments.[15] CIPPIC welcomes the government's recognition of the "fundamental" nature of privacy interests. Canadian law needs this language to afford privacy the weight and legal protection appropriate to a quasi-constitutional right.[16] The wording reflects the international consensus that privacy ranks among the most basic of human rights and fundamental freedoms. Recognizing privacy as a "fundamental right" echoes the *EU Charter of Fundamental Rights*, which establishes binding obligations for EU Member States to protect core categories of rights and freedoms, including privacy.[17] This alignment brings Canada into step with leading democratic peers while grounding its federal privacy framework in international human rights instruments.

The government can better recognize privacy's importance by explicitly adopting a "human rights" approach. Doing so would identify privacy as a core right and freedom while upholding

---

[13] International Civil Liberties Monitoring Group, "Brief on 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*" (25 September 2023); OpenMedia, "Submission to INDU Committee Study of Bill C-27, *The Digital Charter Implementation Act, 2022*" (3 May 2023) [OpenMedia, "Submission on C-27"]; Jane Bailey, Jacquelyn Burkell & Brenda McPhail, "Submissions on Bill C-27" (5 October 2023); Colin Bennett, "Submission on Bill C-27, *Digital Charter Implementation Act*" (26 October 2023); House of Commons, Standing Committee on Industry and Technology, *Evidence*, 44-1, No 92 (26 October 2023) at 1545, 1605 and 1650 (Colin Bennett, Brenda McPhail, Vivek Krishnamurthy); House of Commons, Standing Committee on Industry and Technology, *Evidence*, 44-1, No 94 (2 November 2023) at 1530 (Daniel Konikoff).

[14] Office of the Privacy Commissioner of Canada, "Submission of the Office of the Privacy Commissioner of Canada on Bill C-27, the Digital Charter Implementation Act, 2022" (April 2023) at 5 [OPC, "Submission on Bill C-27"].

[15] Letter from the Honourable François-Philippe Champagne to the Chair of the Standing Committee on Industry and Technology (20 October 2023).

[16] The Supreme Court of Canada has recognized privacy as a fundamental and quasi-constitutional right, and the Federal Court has recognized PIPEDA as fundamental and quasi-constitutional legislation. See *Douez v Facebook*, 2017 SCC 33 at para 105; *Alberta (Information and Privacy Commissioner) v United Food and Commercial Workers, Local 401*, 2013 SCC 62 at para 19; *Nammo v Transunion of Canada Inc*, 2010 FC 1284 at paras 74–75; *Eastmond v Canadian Pacific Railway*, 2004 FC 852 at para 100.

[17] Later incorporated into Charter of Fundamental Rights of the European Union, 7 December 2000, OJ C 326, 26.10.2012, at 391–407; *Treaty of Lisbon amending the Treaty on European Union and the Treaty establishing the European Community*, 13 December 2007, OJ C 306, 17.12.2007 (entered into force 1 December 2009) [*Lisbon Treaty*]; The EU Charter recognizing privacy as "fundamental" likely derives from German law and the notion of "Grundrecht" meaning "basic law" or "fundamental law" or, in French, "droit fondamental." In 1983, the German Federal Constitutional Court recognized an individual's right to informational self-determination as fundamental (*Grundrecht auf informationelle Selbstbestimmung*); Cecília Alberton Coutinho Silva, "The fundamental right of confidentiality and integrity of IT systems in Germany: A call for 'IT Privacy' right in Brazil?" (2021) 2 Intl Cybersecurity LR 253.

Canadian norms and values in line with international human rights principles, including the right to privacy under article 12 of the *Universal Declaration of Human Rights*.[18] CIPPIC calls on the government to articulate clearly in the CPPA that privacy is not merely a "fundamental right", but a "fundamental *human* right".

CIPPIC therefore proposes the following amendments, building on those recommended by the OPC:

> **Preamble**
>
> Paragraph 2: Whereas the protection of the fundamental human right to privacy ~~interests~~ of individuals with respect to their personal information is essential to individual autonomy and dignity and to the full enjoyment of fundamental rights and freedoms in Canada;
>
> Para 3: Whereas Parliament recognizes the importance of the privacy and data protection principles contained in various international instruments including international human rights instruments that recognize privacy as a fundamental and inalienable right;
>
> [...]
> Para 12: And whereas this Act aims to support the Government of Canada's efforts to foster an environment in which Canadians can seize the benefits of the digital and data-driven economy and to establish a regulatory framework that supports and protects Canadian norms and values, including the fundamental human right to privacy;
>
> […]
>
> **Purpose**
>
> **5** The purpose of this Act is to establish […] rules to govern the protection of personal information in a manner that recognizes the fundamental human right to ~~of~~ privacy of individuals with respect to their personal information...

This wording situates Canadian personal information protection within the international human rights framework and places individuals at the centre of the CPPA's object and purpose. Explicitly qualifying privacy as a fundamental human right strengthens the law's constitutional grounding and forecloses interpretive ambiguity, confirming that personal information protection law vindicates human rights.

Finally, Parliament should embed this language in specific provisions of the CPPA, to ensure that organizations and the Tribunal accord privacy due weight when assessing necessary

[18] *Universal Declaration of Human Rights*, UNGA, 3rd Sess, UN Doc A/810 (1948) GA Res 217A (III).

measures and precautions.[19] For example, subsection 12(2) should explicitly require organizations to consider privacy as a fundamental human right:

> **Appropriate Purposes - Factors to consider**
>
> 12(2) The following factors must be taken into account in determining whether the manner and purposes referred to in subsection (1) are appropriate:
>
> > (**a**) the importance of the fundamental human right to privacy.
> >
> > (~~**a**~~ **b**) the sensitivity of the personal information;
> >
> > […]
> >
> > **(e g)** whether the intrusion upon the individual's ~~loss of~~ right to privacy is minimal and is justified by ~~proportionate to~~ the benefits in light of the measures, technical or otherwise, implemented by the organization to mitigate the impacts of the loss of privacy on the individual.

CIPPIC suggests further amendments acknowledging privacy rights as fundamental human rights in subsection 18(3) (see Recommendation 3.3) and subsection 9(2)(d) (see Recommendation 4.3).

2. Strengthen and refine the CPPA's scope

Legislation must protect the human right to privacy clearly and consistently. This requires both guidance on what constitutes "sensitive information" and substantive safeguards that compel organizations to confront the privacy risks inherent in collecting, using, and disclosing Canadians' personal information. These safeguards must extend to anonymized data, which remains vulnerable to re-identification as AI technology advances.[20] Political parties must face the same privacy standards, to preserve Canadians' trust in the integrity of the democratic system.

2.1 Define "sensitive information"

Health, biometric, and genetic data rank among the most sensitive and vulnerable categories of Canadians' personal information. Although organizations may anonymize such data, the re-

[19] As recommended by INDU witnesses Brenda McPhail and Michael Geist; House of Commons, Standing Committee on Industry and Technology, *Evidence*, 44-1, No 92 (26 October 2023) at 1615 and 1710 (Michael Geist, Brenda McPhail).

[20] Alex Hern, "New York Taxi Details Can Be Extracted From Anonymised Data, Researchers Say", *The Guardian* (27 June 2014); Law Commission of Ontario, *Consumer protection in the Digital Marketplace: LCO Consultation Paper* (Toronto: Law Commission of Ontario, 2023) at 73 [LCO, *Consumer Protection*]; House of Commons, Standing Committee on Industry and Technology, *Evidence*, 44-1, No 107 (31 January 2024) at 1805 (Nicolas Papernot).

identification risks for these categories are well documented.[21] The CPPA should define them as "sensitive information," alongside the personal information of minors.

Subsection 2(2) of the CPPA currently specifies that "the personal information of minors is considered to be sensitive information," yet it provides no definition of "sensitive information" itself. The CPPA requires one.[22]

> **Definitions**
>
> **2 (1)** ***Sensitive information*** means personal information for which an individual has a heightened expectation of privacy, or for which collection, use or disclosure creates a heightened risk of harm to the individual.[23]

The CPPA also needs interpretive guidance on "sensitive information" to give both Canadians and organizations clarity about what the term captures. That interpretation must protect Canadians' most private information and align with current international standards such as the EU's GDPR. Such alignment reduces the compliance burden on organizations operating across multiple jurisdictions. CIPPIC accordingly proposes rewriting subsection 2(2) as follows:

> **Interpretation – ~~minors~~ sensitive information**
>
> **2 (2)** For the purposes of this Act, ~~the personal information of minors is considered to be sensitive information~~ sensitive information includes personal information relating to:
>
> **(a)** minors;
>
> **(b)** health, biometric, and genetic information;
>
> **(c)** racial or ethnic origin;
>
> **(d)** political opinion or affiliation;
>
> **(e)** religious or philosophical beliefs;
>
> **(f)** sexuality or sexual orientation;
>
> **(g)** the tracking of an individual's geographic location; or
>
> **(h)** any other information deemed to be sensitive through regulation.

---

[21] House of Commons, Standing Committee on Industry and Technology, *Evidence*, 44-1, No 94 (2 November 2023) at 1530 (Daniel Konikoff); Canadian Civil Liberties Association, "Submission to the Standing Committee on Industry and Technology regarding 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*" (12 September 2023) at 7-8.

[22] See OPC, "Submission on Bill C-27", *supra* note 14.

[23] See Centre for Digital Rights, "Not Fit for Purpose – Canada Deserves Much Better" (28 October 2022) at 11.

2.2 Include a data protection impact assessment framework

A data protection impact assessment (DPIA) framework gives organizations a structured process to identify and minimize the data protection risks their products or services create.[24] DPIAs sit at the heart of the EU's GDPR, which requires them for projects likely to involve "a high risk" to individuals' personal information.[25] The UK's *Data Protection Act, 2018* similarly requires organizations to conduct a DPIA before any data processing that poses "a high risk to the rights and freedoms of individuals."[26] The assessment must describe the processing operations, assess the risks to data subjects' rights and freedoms, and specify the measures and safeguards the organization will deploy to counter those risks.[27]

The CPPA contains a loosely analogous framework under its exceptions-to-consent provisions, which requires organizations to identify potential adverse effects of data collection, mitigate or eliminate those effects, and comply with any prescribed requirements.[28] That framework, however, applies only to data collected under the section 18 exceptions. Organizations that obtain explicit consent to collect, use, and disclose Canadians' most private information face no obligation to proactively assess the adverse effects such collection may cause, or to take steps to mitigate those risks. The only data protection safeguards that would apply are those in the privacy management program under section 9. That program requires only that organizations "put in place [...] policies, practices and procedures respecting […] the protection of personal information" in a manner that "take[s] into account the volume and sensitivity of the personal information."[29] This broad and ambiguous standard is insufficient given the highly personal nature of sensitive or high-risk information. It also fails to give organizations concrete guidance on what risks to consider when handling sensitive or high-risk information or what steps they must take to counter these risks.

Parliament should therefore expand the privacy management program in section 9 to impose more stringent requirements on organizations that collect, use, and disclose Canadians' sensitive or high-risk information, regardless of whether they gathered that data under the section 18 exceptions to consent. Adopting the DPIA framework would harmonize Canada's approach with those of the EU and UK and address concerns that INDU witnesses have raised.[30] CIPPIC proposes the following amendments to section 9:

---

[24] UK, Information Commissioner's Office, *Guide to the General Data Protection Regulation (GDPR)* (October 2022) at 201.
[25] Ben Wilford, "Data Protection Impact Assessment".
[26] As determined by the "nature, scope, context and purposes of the data processing", see *Data Protection Act*, *supra* note 4, s 64.
[27] *Ibid*; California Design Code, *supra* note 4 at §1798.99.31(a).
[28] CPPA, *supra* note 2, s 18(4).
[29] *Ibid*, ss 9(1)(a), 9(2).
[30] See House of Commons, Standing Committee on Industry and Technology, *Evidence*, 44-1, No 92 (26 October 2023) at 1545, 1600 (Colin Bennett, Vivek Krishnamurthy).

Volume ~~and sensitivity~~

9 (2) In developing its privacy management program, the organization must take into account the volume and sensitivity of the personal information under its control.

Data protection impact assessments

(3) In developing its privacy management program, organizations involved in the collection, use or disclosure of sensitive or high-risk information must develop and implement a data protection impact assessment (DPIA) framework that:

(a) assesses the potential risks to the rights and freedoms of data subjects in relation to

(i) the nature, scope, context, purpose and volume of the data collected, used or disclosed,

(ii) the necessity and proportionality of the collection, use or disclosure in relation to the purpose of these activities; and

(iii) the sensitivity of the personal information, including whether it belongs to a minor;

(b) identifies any potential adverse effect on an individual or group that is likely to result from the collection, use or disclosure of their personal information;

(c) takes reasonable measures to reduce the likelihood that the potential risks and adverse effects identified under paragraphs 9(3)(a) and (b) will occur or, whenever possible, to mitigate or eliminate these risks, through policies, practices and procedures that include but are not limited to

(i) information storage and security safeguards; and

(ii) proactive measures to inform individuals in the case of security breaches involving their personal information;

(d) is updated either every 5 years or whenever the organization's policies on the collection, use or disclosure of personal information undergo substantial changes, or whenever a material change occurs in processing, technology, data source, purpose, affected population or risk, whichever occurs first; and

(e) complies with any prescribed requirements.

The CPPA should also define "adverse effect" to give organizations working with sensitive or high-risk information clear guidance as they implement DPIA requirements. The definition should not be confined to measurable economic, physical, or psychological injury.[31] Privacy infringements may diminish autonomy, dignity, equality, security, and democratic participation without producing immediate or readily quantifiable harm. The definition should therefore capture direct and indirect effects, individual and collective effects, and present (and reasonably foreseeable) future risks arising from the collection, use, or disclosure of personal information:

> **Definitions**
>
> **2 (1)** ***Adverse effect*** means any reasonably foreseeable detrimental effect on an individual's rights, interests, freedoms or well-being, including but not limited to:
>
> (a) physical or psychological harm;
>
> (b) financial loss or economic disadvantage;
>
> (c) reputational harm;
>
> (d) loss of privacy, confidentiality or control over personal information;
>
> (e) discrimination, profiling or unfair differential treatment;
>
> (f) manipulation, coercion or impairment of individual autonomy or decision-making;
>
> (g) chilling effects on lawful activities or the exercise of rights and freedoms;
>
> (h) increased risks arising from unauthorized access, re-identification or future misuse of personal information; and
>
> (i) any other material interference with an individual's dignity, equality, security or fundamental rights.

Finally, direct engagement between individuals and the organizations that collect their personal information is essential to responsible innovation and mutual trust.[32] Such engagement ensures that societal norms and values shape organizations' privacy policies, keeping organizations responsive to the people whose data they handle.[33] In time, it may yield a more sustainable, marketable, and socially desirable pipeline of innovation.[34]

> **Access — privacy management program**
>
> **10 (1)** An organization must, on request of the Commissioner or of the individual whose personal information is being collected, used or disclosed,

[31] See Ido Kilovaty, "Psychological Data Breach Harms" (2023) 23:1 North Carolina JL & Tech 1.
[32] Ruggiu *et al*, *supra* note 12; Marc van Lieshout & Sophie Emmert, "RESPECT4U – Privacy as Innovation Opportunity" (Paper delivered at the Proceedings of the 6th Annual Privacy Forum) (2018) 6 Annual Privacy Forum 43.
[33] Bernd Carsten Stahl, "Responsible Research and Innovation: The Role of Privacy in an Emerging Framework" (2013) 40:6 Science & Pub Pol'y 708 at 709.
[34] *Ibid*; Ruggiu *et al*, *supra* note 12 at 324.

provide the Commissioner or that individual with access to the policies, practices and procedures that are included in its privacy management program.

2.3 Preserve regulatory oversight of anonymized information

Privacy law should recognize anonymization as a valuable privacy-protective technique without treating it as sufficient reason to remove information wholly from regulatory oversight. Whether information meets the statutory standard for anonymization is a technical and contextual question, and erroneous or overstated claims of anonymization may expose individuals to re-identification and other privacy risks. Researchers have repeatedly demonstrated that "anonymized data, including home addresses, income, and movement patterns, can be reverse engineered or combined with other data to re-identify individuals."[35] The United States Federal Trade Commission points to research showing that, in some instances, researchers could uniquely identify 95% of a dataset of 1.5 million individuals, roughly the current population of Manitoba.[36] CIPPIC, alongside leading voices in internet policy, has raised serious concerns about this risk, particularly for sensitive personal information such as medical records and children's data.[37]

Excluding anonymized data from the CPPA also contradicts recent recommendations from the ETHI Standing Committee of the House of Commons.[38] ETHI recommended that Parliament amend federal laws to render them "applicable to the collection, use, and disclosure of de-identified and aggregated data."[39] Excluding anonymized information entirely from the CPPA would also deprive the Privacy Commissioner of a meaningful role in determining whether organizations have properly applied the statutory anonymization standard. As Dr. Teresa Scassa has explained, CPPA s 6(5) currently falls short of that standard because "aggregated data" is generally understood to mean data that organizations have anonymized.[40] Information described as anonymized or aggregated should not automatically fall beyond governance merely because an organization applies that label. The Act should therefore permit the Commissioner to review organizations' anonymization practices, assess whether information meets the statutory standard, and require corrective action where it does not.

CIPPIC accordingly proposes replacing subsection 6(5), which states that the CPPA "does not apply in respect of personal information that has been anonymized," with the following:

---

[35] Alex Hern, "New York Taxi Details Can Be Extracted From Anonymised Data, Researchers Say", *The Guardian* (27 June 2014); LCO, *Consumer Protection*, *supra* note 20.
[36] Kristin Cohen, "Location, Health, and Other Sensitive Information: FTC Committed to Fully Enforcing the Law Against Illegal Use and Sharing of Highly Sensitive Data" (12 July 2022).
[37] Teresa Scassa, "Anonymization and De-identification in Bill C-27" (6 July 2022); House of Commons, Standing Committee on Industry and Technology, *Evidence*, 44-1, No 92 (26 October 2023) at 1605, 1620-1625 (Brenda McPhail).
[38] Scassa, "Anonymization and De-identification in Bill C-27", *supra* note 37.
[39] *Ibid*; House of Commons, Standing Committee on Access to Information, Privacy and Ethics, Collection and Use of Mobility Data by the Government of Canada and Related Issues (May 2022) (Chair: Pat Kelly), 44-1, 4th Report.
[40] Scassa, "Anonymization and De-identification in Bill C-27", *supra* note 37.

For greater certainty

6 (5) Except as provided in subsection (6), ~~For greater certainty,~~ this Act does not apply in respect of personal information that has been anonymized in accordance with this Act and the regulations.

Commissioner's oversight

6 (6) Sections 9, 10, 74, 97 and 98 apply in respect of an organization's practices for anonymizing personal information, including its compliance with the definition of "anonymize" and any prescribed technical and administrative requirements.

6 (7) For greater certainty, the Commissioner may audit or otherwise review an organization's anonymization practices and determine whether information represented by the organization as anonymized meets the requirements of this Act.

These amendments preserve the CPPA's exclusion for information that genuinely satisfies the statutory anonymization standard, while ensuring that an organization cannot place information beyond the Act merely by declaring it anonymized. They give the Privacy Commissioner express authority to examine anonymization practices, verify compliance with the statutory definition and applicable regulations, and require corrective action where the standard has not been met.[41]

This oversight becomes especially important if Parliament lowers the statutory threshold for anonymization. A less exacting standard may facilitate socially beneficial uses of data, but it also increases the need for independent review, proportionate safeguards, and accountability for residual re-identification risk. The growing risk of re-identification, which advances in AI make increasingly feasible, demands a regulatory approach to anonymization that can keep pace with technological change.[42] The Commissioner should therefore have authority to audit organizations' anonymization methods and issue guidance on generally accepted practices, while binding technical requirements should be established through legislation or regulation.

A well-designed regulatory framework, developed in genuine consultation with stakeholders, would encourage responsible anonymization and give organizations greater certainty about the applicable standard. The Privacy Commissioner should issue interpretive and technical guidance, while regulations should establish any binding minimum requirements and proportionate safeguards for the processing, storage and use of anonymized information. The framework could also recognize appropriate public-interest applications without leaving anonymization practices beyond independent scrutiny.

[41] Scassa, "Anonymization and De-identification in Bill C-27", *supra* note 37.
[42] House of Commons, Standing Committee on Industry and Technology, *Evidence*, 44-1, No 107 (31 January 2024) at 1805 (Nicolas Papernot).

2.4 Bring federal political parties under the CPPA

Nothing justifies continuing to exempt Canada's federal political parties from the privacy laws that govern other organizations. As Dr. Michael Geist testified to INDU, the government cannot "credibly argue that privacy is a fundamental right and then claim that it should not apply in a robust manner to political parties."[43]

The more permissive privacy law that applies to political parties under the *Canada Elections Act* fails to adequately safeguard Canadians' trust in the integrity of the democratic system.[44] Misuse of personal information poses grave risks to Canadian democracy: parties can target individuals based on their data and process it with increasingly sophisticated AI. Failing to scope political parties into the CPPA also conflicts with the Office of the Information and Privacy Commissioner of British Columbia's finding that the province's *Personal Information Protection Act* applies to political parties with only limited exceptions.[45]

The CPPA's exclusion of political parties leaves Canada behind emerging international norms of political accountability and transparency. Recognizing the risks inherent in political dealings with personal information, Canada's democratic peers have chosen to regulate political parties under their privacy laws.[46] The EU's GDPR, for example, applies to political parties with few exceptions.[47]

CIPPIC accordingly joins the Centre for Digital Rights, OpenMedia, and others in urging Parliament to amend subsection 6(1) to expressly include political parties within the CPPA's scope by adding a new paragraph that reads:

> **Application**
>
> **6 (1)** This Act applies to every organization in respect of personal information that
>
> > […] (c) is collected, used or disclosed by a political party, a candidate, an electoral district association, or a nomination contestant in connection with electoral activities.[48]

Subsection 2(1) should also define "political party," "candidate," "electoral district association," and "nomination contestant," drawing on the *Canada Elections Act*, along with "electoral activities," meaning "any activities related to promoting a federal political party at any time, whether during a formal election period or otherwise."[49]

---

[43] House of Commons, Standing Committee on Industry and Technology, *Evidence*, 44-1, No 92 (26 October 2023) at 1550 (Michael Geist).
[44] *Canada Elections Act*, SC 2000, c 9.
[45] Centre for Digital Rights, "Not Fit for Purpose", *supra* note 23 at 10.
[46] OpenMedia, "Thousands protest government plan to exclude federal political parties from Canadian privacy laws" (2 May 2023).
[47] Centre for Digital Rights, "Not Fit for Purpose", *supra* note 23 at 10.
[48] *Ibid*; OpenMedia, "Submission on C-27", *supra* note 13 at 17.
[49] Centre for Digital Rights, "Not Fit for Purpose", *supra* note 23 at 10.

3. Place individuals at the centre of consent and its exceptions

Meaningful consent is the cornerstone of Canadian data protection law.[50] It is fundamental to privacy because it allows individuals to control who receives their personal information and how others use it.[51] This exercise of choice and autonomy in turn underpins Canadian values and democracy, and respects human dignity.[52]

Privacy laws that ensure meaningful consent build consumer trust and support economic growth rather than stifling innovation. Effective privacy laws benefit both individuals and organizations: when individuals trust how organizations manage their information, they more readily support the innovative goods and services that handle it.[53] A rights-based approach to consent aligns with the government's objectives to enable responsible innovation and enhance Canadians' control and consent.

3.1 Ensure consent remains meaningful

The CPPA's proposed consent and exception framework fails to preserve protections that PIPEDA currently provides, downgrading organizations' consent obligations. Under PIPEDA, "the consent of an individual is only valid if it is reasonable to expect that an individual … *would understand* the nature, purpose and consequences of the collection, use or disclosure of the personal information to which they are consenting."[54] In contrast, Bill C-27 only requires that the organization "*provides*" the relevant information in "plain language."[55] This new standard is more passive and permissive than PIPEDA's requirement that individuals "would understand" the implications of their consent. It downgrades digital consent at a time when technological change places privacy at greater risk.[56]

To avoid this erosion of consent, CIPPIC proposes re-introducing the "would understand" wording into CPPA subsection 15(3):

> **Information for consent to be valid**
>
> **15 (3)** The individual's consent is valid only if, at or before the time that the organization seeks the individual's consent, it ~~provides the individual with the following information:~~
>
> (a) provides the individual with the following information; and
>
> […]

[50] Teresa Scassa, "Bill C-27's Take on Consent: A Mixed Review" (4 July 2022); Office of the Privacy Commissioner of Canada Policy and Research Group, "Privacy and consent: A discussion paper exploring potential enhancements to consent under the *Personal Information Protection and Electronic Documents Act*" (Gatineau, QC: Office of the Privacy Commissioner, 2016).
[51] *Ibid* at 2.
[52] *Ibid*.
[53] OPC, "Submission on Bill C-27", *supra* note 14.
[54] *PIPEDA*, *supra* note 2, s 6.1 [emphasis added].
[55] CPPA, *supra* note 2, s 15(3)-(4) [emphasis added].
[56] OpenMedia, "Submission on C-27", *supra* note 13 at 7; Scassa, "Bill C-27's Take on Consent", *supra* note 50.

(b) is reasonable to expect that the individual would understand this information.

[…]

For greater certainty

15 (8) Criteria on when it is reasonable for an organization to expect that an individual understands the information provided to them under subsection 15(3)(a) is subject to the regulations and any guidance provided by the Office of the Privacy Commissioner.

3.2 Remove the ability to imply consent

Implied consent is a "dated idea that creates confusion for both [individuals] and businesses" and the CPPA should not permit it.[57] Witnesses and stakeholders have criticized the implied consent regime in subsections 15 (5) and (6) as unnecessary and confusing when read alongside the exceptions to consent for "business activities" and "legitimate interests" under subsections 18(2) and (3).[58] The GDPR does not permit the collection, use or disclosure of personal information based on implied consent, and PIPEDA never paired it with the broad "legitimate interest" exception the CPPA introduces.[59] Leaving the implied consent provisions in the CPPA enables organizations to skirt the guardrails built into subsections 18(2) and (3) and creates confusion about their obligations.[60]

Form of consent

15 (5) Consent must be expressly obtained ~~unless, subject to subsection (6), 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 that is to be collected, used or disclosed~~.

~~**Business activities**~~ **Inapplicability of implied consent**

(6) It is not appropriate to rely on an individual's implied consent ~~if their personal information is collected or used for an activity described in subsection 18(2) or (3)~~.

3.3 Make exceptions to consent easy for individuals to understand

Compared to PIPEDA, the CPPA's list of exceptions is "expanded and presented in a way that prioritizes business organizations over individuals looking to inform themselves about their

---

[57] House of Commons, Standing Committee on Industry and Technology, *Evidence*, 44-1, No 92 (26 October 2023) at 1545 (Colin Bennett).

[58] Centre for Digital Rights, "Not Fit for Purpose", *supra* note 23 at 5; Teresa Scassa, "Comments to INDU Committee on the Consumer Privacy Protection Act (in Bill C-27)" (2 November 2023); House of Commons, Standing Committee on Industry and Technology, *Evidence*, 44-1, No 92 (26 October 2023) at 1550, 1645 (Michael Geist, Vivek Krishnamurthy); Bailey, Burkell & McPhail, "Submissions on Bill C-27", *supra* note 13 at 8-9.

[59] CPPA, *supra* note 2, s 18(3); Scassa, "Comments to INDU Committee", *supra* note 58.

[60] Scassa, "Comments to INDU Committee", *supra* note 58.

privacy rights."[61] This primacy of commercial interests across this regime (ss 18-52) sends the interpretive message that business interests outweigh individual privacy.[62]

Parliament should restructure the exception regime to be more user-centric, so that individuals looking to the CPPA for guidance can navigate it more easily. Absent a restructuring, the Office of the Privacy Commissioner should provide Canadians with clear and meaningful guidance on how to interpret the CPPA's exceptions to consent, and on what they can do if they are concerned that an organization has failed to comply.

3.4 Prioritize fundamental rights over business interests

Parliament must bring the legitimate interest exception to consent under subsection 18(3) within a human rights framework.[63] Currently, the subsection would allow organizations to collect or use an individual's personal data without consent if three conditions are met: the organization's legitimate interest "outweighs any potential adverse effect on the individual"; a reasonable person would expect this collection or use; and the organization does not use the personal information to influence the individual's behaviour or decisions.[64] This approach is problematic because it requires the organization to conduct "a risk assessment performed by the company rather than a judgment made about the human rights of individuals to control their personal information."[65] This imbalance of power lets the organization decide what constitutes a legitimate interest without consulting the individual or considering their rights. The ambiguity about what constitutes a "legitimate interest" also raises concerns about how broadly section 18(3) could apply.[66]

Like section 18(3), GDPR article 6(1)(f) allows an organization to process individuals' personal data without their explicit consent when doing so "is necessary for the purposes of ... legitimate interests."[67] However, the GDPR qualifies legitimate interest by requiring that it not be "overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child."[68] This recognizes the power imbalance inherent in letting organizations declare their own legitimate interests, and places the onus on them to show they have weighed that interest against the rights and freedoms of the individual, especially a child.

Parliament must amend the CPPA's legitimate interest exception so that organizations' business interests cannot override individuals' rights and freedoms, even where the organization anticipates no "adverse effect on the individual." Given children's heightened

---

[61] OpenMedia, "Submission on C-27", *supra* note 13 at 7.
[62] *Ibid*.
[63] House of Commons, Standing Committee on Industry and Technology, *Evidence*, 44-1, No 92 (26 October 2023) at 1545 (Colin Bennett).
[64] CPPA, *supra* note 2, s 18(3).
[65] House of Commons, Standing Committee on Industry and Technology, *Evidence*, 44-1, No 92 (26 October 2023) at 1545 (Colin Bennett).
[66] Scassa, "Bill C-27's Take on Consent", *supra* note 50.
[67] GDPR, *supra* note 3, art 6(1)(f).
[68] *Ibid*.

vulnerability, the exception should permit the collection or use of a child's personal information for an organization's legitimate interest only when doing so is in the best interest of the child (see Recommendation 4.1). Given the ambiguity of "legitimate interests" and concerns about abuse of the provision, subsection 18(3) should be subject to regulations that provide additional interpretive detail. Such regulations would provide organizations with clarity about what is and is not a valid legitimate interest, and give the government flexibility to update the standard as technology advances and evidence emerges on how organizations use the provision.

> **Legitimate interest**
>
> **18 (3)** Except where such interests are overridden by the interests or fundamental rights and freedoms of the individual, such as the human right to privacy, a~~A~~n organization may collect or use an individual's personal information without their knowledge or consent if the collection or use is made for the purpose of an activity in which the organization has a legitimate interest that outweighs any potential adverse effect on the individual resulting from that collection or use and,
>
> **[...]**
>
> **(d)** if the personal information belongs to a minor, it is in the best interests of the child to have their personal information collected or used without consent; and
>
> **(e)** the collection or use complies with any prescribed regulations.

Note: Additional amendments using "best interest of the child" language are proposed in Recommendation 4.1, and additional changes to section 18 are proposed under Recommendation 3.4 and Recommendation 5.2.

3.5 Increase transparency and accountability in cases of exceptions to consent

Organizations relying on the section 18 exceptions should explain to the public how they decide to assume consent. They owe this transparency to the public, not only to the Privacy Commissioner, because they are overlooking the public's consent. Organizations that assume consent should also bear a heightened burden to mitigate the risks that accompany data collection, use, and disclosure.

Engagement between individuals and the organizations that handle their data strengthens responsible innovation and trust.[69] Organizations that assume consent should respond to individuals who ask what risk assessment and mitigation measures the organization is taking to protect their privacy. Embedding public accountability in the use of consent exceptions will protect trust between individuals and organizations, encourage responsible use of those exceptions, and inform how organizations develop their section 18 records of assessment.

[69] Ruggiu *et al*., *supra* note 12; Lieshout & Emmert, *supra* note 32, pp 43-60.

Organizations relying on section 18 exceptions should therefore, on request, release information about their assessment of potential adverse effects and the measures they have taken to mitigate and eliminate those effects under subsection (4):

> **Record of assessment**
> **18 (5)** The organization must record its assessment of how it meets the conditions set out in subsection and must, on request, provide a copy of the assessment to the Commissioner or to the individual whose personal information has been collected, used or disclosed.

4. Strengthen protections for children's privacy

Children deserve protection from how corporations collect and commercialize their data, particularly as they spend increasing amounts of time online. The current draft of the CPPA leaves many gaps in protecting children's privacy. If enacted in its current form, "[t]he *CPPA* risks becoming outdated…because it falls short compared to other children's privacy protection laws globally."[70]

4.1 Include "best interest of the child" language

The "best interest of the child" should be the primary consideration in all design choices by organizations developing or providing online services for children. The UK Code and California Design Code expressly state this, but the CPPA does not. The California Design Code further states that "[i]f a conflict arises between commercial interests and the best interests of children, companies should prioritize the privacy, safety, and well-being of children over commercial interests."[71] Recognizing the "best interests of the child" also aligns with Canada's international legal obligations under Article 3 of the *UN Convention on the Rights of the Child*, which states "[i]n all actions concerning children…the best interests of the child shall be a primary consideration."[72] CIPPIC therefore recommends defining "best interest of the child" in the CPPA across four provisions: section 2(1) (the definition); section 4(a) (rights and recourses that may be exercised on behalf of a minor or by the minor); section 12(2) (factors to consider for appropriate purposes); and section 55(2) (reasons why an organization may refuse a request to dispose of personal information).

> **Definitions**
>
> **2(1)** ***best interests of the child*** means prioritizing the welfare of children as the primary consideration and acting to protect this welfare first and foremost.

[70] George Hua and Vivek Krishnamurthy, "Every Child Left Behind: How Bill C-27 Fails to Adequately Protect the Privacy Rights of Canada's Children" (Ottawa: Samuelson-Glushko Canadian Internet Policy and Public Interest Clinic, 2023).
[71] California Design Code, *supra* note 4, s 1798.99.29(b).
[72] Convention on the Rights of the Child, 20 November 1989, 1577 UNTS 2 (entered into force 2 September 1990) at 45 [UNCRC] (Canada signed and ratified the UNCRC in 1991).

Appropriate purposes - Factors to consider

12 (2) The following factors must be taken into account in determining whether the manner and purposes referred to in subsection (1) are appropriate:

> […] **(e)** when involving the personal information of a minor, whether the collection, use or disclosure of information are in the best interests of the child;
>
> **(~~d~~ f)** […].

Disposal at individual's request - Exception

55 (2) An organization may refuse a request to dispose of personal information in the circumstances described in paragraph (1)(b) or (c) if

> **(a)** disposing of the information would result in the disposal of ~~personal information about another individual and the information is not severable;~~
>
> > **(i)** personal information about another individual and the information is not severable, or
> >
> > **(ii)** personal information about a child and such disposal is not in the best interest of the child;
>
> **(b)** […]

In addition to these amendments, CIPPIC proposes including "best interests of the child" language in subsection 4(1)(a) (Recommendation 4.4), subsection 9(3)(b)(ii) (Recommendation 4.2), and subsection 18(3)(c) (Recommendation 3.3).

4.2 Ensure children's privacy is considered during data protection impact assessments

The UK Code requires a DPIA before an organization launches any new online service for children, or makes significant changes to an existing service that children access.[73] This applies to all "information society services likely to be accessed by children", even if children are not the targeted audience or user.[74] The UK Code generally requires large organizations whose online services are likely to be accessed by children to seek opinions on their data protection policies.[75] They might gather feedback from existing users, carry out a public consultation, or contact relevant children's rights groups for their views. These consultations should seek feedback on, among other things, children's ability to understand how their data is used and how the organization explains its privacy policies. Similarly, the California Design Code

[73] UK Code, *supra* note 4 at 27.
[74] Information Commissioner's Office, "Introduction to the Children's Code".
[75] UK Code, *supra* note 4 at 35.

requires an organization to complete a DPIA before it offers an online service or product to the public, and to review that DPIA every two years.[76]

To ensure adequate privacy protections for minors and harmonize with these international best practices, section 9 of the CPPA should require organizations that are likely to be dealing with children's personal information to review their DPIAs more frequently than those that do not. It should also require large organizations to include a public consultation in their DPIAs.[77] Parliament should therefore adopt the following amendment, in addition to the DPIA requirements suggested under Recommendation 2.2:

> **Data protection impact assessments – children's personal information**
>
> **9 (4)** When the organization is likely to collect, use or disclose the personal information of children, the DPIA conducted under subsection (3) must
>
> > **(i)** be reviewed every 2 years or whenever the organization's policies on the collection, use or disclosure of personal information undergo substantial changes, whichever occurs first; and
> >
> > **(ii)** if the organization has 500 or more paid employees, solicit public feedback on its data protection policies and procedures that includes, but is not limited to, children's ability to understand the organization's privacy policies and data usage.

4.3 Require privacy settings be set to "high" by default

The UK Code and California Design Code both require online services and products that children are likely to access to default to "high" privacy settings. If the service or product has a different privacy setting, the provider must show how this is in the "best interest" of children.[78] The CPPA should similarly require services and products to default to the highest privacy setting if children are likely to access them. The highest privacy settings turn off geo-location tracking and prohibit optional uses of personal data obtained through the service or product.[79]

To achieve this, the CPPA should define "default" and add provisions to section 9 that set out the expected default privacy settings for services and products that children access:

> **Definitions**
>
> **2 (1)** ***Default*** means a preselected option adopted by the business during commercial activity.

---

[76] California Design Code, *supra* note 4 at 1798.99.31(a).
[77] Innovation, Science and Economic Development Canada, *Key Small Business Statistics, 2022* (Ottawa: Innovation, Science and Economic Development Canada Small Business Branch, 2022)
[78] California Design Code, *supra* note 4, s 1798.99.31(a)(6).
[79] Hua and Krishnamurthy, "Every Child Left Behind", *supra* note 70.

Privacy management program

9 (1) Every organization must implement and maintain a privacy management program that includes the policies, practices and procedures the organization has put in place to fulfill its obligations under this Act, including policies, practices and procedures respecting

> […] **(e)** when the individual whose personal information is being collected, used or disclosed is known to be a child, suspected of being a child, or is likely to be a child; the default implementation of high privacy protection settings which
>
> > (i) permit the collection, use or disclosure of only that personal information which is necessary;
> >
> > (ii) disable geo-location tracking and any optional uses of personal data, including personalization settings;
> >
> > (iii) prohibit profiling based on an individual's previous behavior, browsing history, or similarity to others;
> >
> > (iv) prevent the collection, use or disclosure of the personal information to any third parties; and
> >
> > (vi) otherwise conforms to the regulations.

[…]

Modifications of default high privacy protection

9 (5) The high privacy protections required by default under subsection 9(1)(e) may be lowered only if

> (a) they are lowered only as much as is necessary; and
>
> (b) the organization can demonstrate that
>
> > (i) it has appropriate safeguards in place to protect children, and
> >
> > (ii) it is in the best interests of the child to modify the default privacy protections.

4.4 Provide a framework to determine a minor's capacity to exercise their rights and recourses

The rights and recourses under the CPPA may be exercised "on behalf of the minor by a parent, guardian or tutor, unless the minor wishes to exercise those rights and recourses and is capable

of doing so."[80] The CPPA, however, provides no guidance for determining whether a minor is capable of exercising those rights independently or for resolving a disagreement between the minor and their parent, guardian or tutor. Without statutory guidance, organizations may be required to assess a minor's capacity on an ad hoc basis. Organizations may lack the information and expertise needed to make that assessment consistently. The absence of clear criteria may also produce uncertainty for minors seeking to exercise rights of access, correction, disposal or complaint.

The CPPA should therefore establish a framework for determining whether a minor is capable of exercising the rights and recourses available under the Act:

> **Authorized representatives**
>
> **4 (1)** The rights and recourses provided under this Act may be exercised
>
> > **(a)** on behalf of a minor by a parent, guardian or tutor who is acting in the best interests of the child unless the minor wishes to personally exercise those rights and recourses and is capable of doing so;
> >
> > […]
>
> **For greater certainty**
>
> **(2)** For greater certainty, the capacity of a minor to exercise their rights and recourses under this Act is assessed based on
>
> > **(a)** maturity, which assesses the minor's ability to reasonably and independently express their views, in conjunction with age;
> >
> > **(b)** sufficient understanding of the issue to formulate their own views, which requires knowing the possible available options and the consequences of their decision; and
> >
> > **(c)** impact of the decision on the minor.

5. Combat dark patterns

Researchers have long recognized nudges as user-experience design choices that subtly direct consumers to make desired decisions. An example of a nudge is Google's suggestion to use a strong password when creating a new account. However, dark patterns emerge when these nudges become manipulative and consumers cannot avoid them.

The CPPA acknowledges the crux of dark patterns, which it describes as "deceptive and misleading practices."[81] However, dark patterns go further; they prey on users' cognitive biases and impair their decision-making. The CPPA must address dark patterns, both to void any

[80] CPPA, *supra* note 2 at s 4(a).
[81] *Ibid*, s 16.

consent that organizations obtain through them, and to hold those organizations accountable and bar them from using such practices.

California and Colorado have enacted consumer privacy legislation that explicitly bans dark patterns, and the U.S. Federal Trade Commission has vowed to bring actions against organizations that "trick and trap" consumers into subscription services.[82] The European Data Protection Board has published guidelines that help both consumers and developers detect dark patterns that violate the EU's GDPR.[83]

5.1 Define "dark patterns"

Describing dark patterns as "deceptive and misleading practices" is insufficient to hold organizations accountable or bar them from the practice.[84] The CPPA captures the underlying conduct, but never defines "dark patterns" explicitly, unlike California and Colorado. CIPPIC accordingly proposes adding the following definition to section 2(1):

> **Definitions**
> **2 (1)** ***dark patterns*** mean a user interface or user experience designed or manipulated with the effect of subverting or impairing user autonomy, decision-making, or choice.

5.2 Recognize that consent obtained through dark patterns is void

Parliament must amend section 16 of the CPPA to refer expressly to dark patterns and to provide that any consent an organization obtains through them is void. It should also amend section 18 to ban organizations from using dark patterns in their business activities.

> **Dark patterns**
>
> **16** An organization must not obtain or attempt to obtain an individual's consent by providing false or misleading information or using deceptive or misleading practices, including the use of dark patterns. Any consent obtained under those circumstances is invalid.
>
> **Business activities**
> **18 (1)** An organization may collect and use an individual's personal information without their knowledge or consent if the collection or use is made for the purpose of a business activity described in subsection (2) and
>
> **(a)** a reasonable person would expect the collection or use for such an activity; ~~and~~

[82] Federal Trade Commission, "FTC to Ramp up Enforcement against Illegal Dark Patterns that Trick or Trap Consumers into Subscriptions" (October 28, 2021).
[83] European Data Protection Board, *Guidelines 3/2022 on Dark Patterns in social media platform interfaces: How to recognize and avoid them* (2022).
[84] CPPA, *supra* note 2 at s. 16.

> **(b)** the personal information is not collected or used for the purpose of influencing the individual's behaviour or decisions;
>
> **(c)** the personal information is not collected through the use of dark patterns;
>
> [...]

Note: see additional amendments proposed to subsection 18(1) under Recommendation 3.3.

6. Create a framework for managing data brokers

Third-party organizations who base their business models on collecting, acquiring, aggregating, analyzing, licensing, and commercializing personal information operate extensively in Canada.[85] These "data brokers" collect personal information to create digital dossiers about individuals, and often run those dossiers through predictive analytics to forecast each individual's characteristics or future behaviour.[86] Data brokers then sell or otherwise profit from the results of this analysis, and the data itself, often without the knowledge of the individuals whose personal information is involved. The contemporary data broker model largely monetizes derived products (*i.e.*, profiles, scores, audiences, inferences, identity graphs, *etc.*) rather than simply buying and selling raw datasets. Currently, the global data brokerage market is valued at more than $300 billion USD, with estimates predicting it will reach roughly USD $500 billion by 2030.[87] This multi-billion-dollar economy rests on trading in personal information, often without consent, and profiting from it.[88]

Data brokers raise pressing concerns about consent because they often operate as third parties collecting personal information indirectly.[89] In such circumstances, obtaining meaningful consent is especially difficult, particularly where the intended use of personal information is a secondary purpose that may exceed what a reasonable individual would expect given the circumstances of the original disclosure.[90] Commentators have criticized data brokers for offering no tangible benefits to individuals despite exploiting their data, often using deceptive

---

[85] Office of the Privacy Commissioner of Canada, "Data Brokers: A Look at the Canadian and American Landscape" (September 2014) at 9; Samuelson-Glushko Canadian Internet Policy and Public Interest Clinic, "On the Data Trail: How detailed information about you gets into the hands of organizations with whom you have no relationship" (April 2006).

[86] Hannah Ruschemeier, "Data Brokers and European Digital Legislation" (2023) 9 European Data Protection LR 27 at 30.

[87] Transparency Market Research values the market at USD 462.4 billion by 2031, while Knowledge Sourcing Intelligence predicts a USD 545.431 billion valuation by 2028; "Data Brokers Market Estimated to Reach US$ 462.4 billion by 2031, TMR Report", *Globe News Wire* (1 August 2022); Knowledge Sourcing Intelligence, *Global Data Broker Market Size, Share, Opportunities, COVID-19 Impact, And Trends By Data Type (Consumer Data, Business Data), By End-User (BFSI, Retail, Automotive, Construction, Others), And By Geography - Forecasts From 2023 To 2028*, Report Code KSI061611226 (Knowledge Sourcing Intelligence, 2023).

[88] OpenMedia, "Submission on C-27", *supra* note 13 at 15.

[89] Ruschemeier, *supra* note 86 at 30-31.

[90] CIPPIC, "On the Data Trail", *supra* note 85 at 5.

practices to do so, and concealing that they sell personal information commercially.[91] For example, the Canadian multinational Thomson Reuters not only owns Westlaw Canada and other legal products and services, but also generates income by aggregating personal information from individuals' financial records, utility bills, social media, and other sources. It then sells this information to customers such as the US Immigration and Customs Enforcement (ICE). ICE uses this data to target undocumented immigrants for detention and deportation.[92] In a related but less covert practice, researchers at Duke University found data brokers advertising data about current and former military personnel.[93]

Bad-faith data brokers raise serious human rights and safety concerns. Beyond violating individuals' human right to privacy, their mass collection and use of personal data heightens the risk that this information will be used for unfair or unethical purposes, including profiling and discrimination against individuals on grounds that violate human rights law.[94] Large accumulations of personal information also become targets for cybercriminals and identity thieves.[95]

Despite this, the CPPA does not address data brokers. Instead, the CPPA's general rules on personal information apply to data brokers as they do to any other organization.[96] Although the CPPA's general obligations apply to data brokers, section 51 permits organizations to collect, use, or disclose prescribed publicly available personal information without an individual's knowledge or consent, leaving individuals with significantly reduced control over how data brokers acquire and commercialize that information.[97]

A modern privacy regime must instead offer a framework that promotes the responsible use of data alongside innovation, especially for organizations whose profit models depend on collecting and processing large volumes of personal information through third-party arrangements. The US has proposed such legislation at the federal level (the *American Data Privacy and Protection Act*), and state-level legislation in California and Vermont already regulate data brokers.[98] Similarly, although the GDPR does not specifically regulate data brokers, its generally applicable requirements concerning lawful processing, transparency,

---

[91] Bryan Short, "Everything you need to know about data brokers" (23 June 2022).
[92] *Ibid*.
[93] Justin Sherman et al., "Data Brokers and the Sale of Data on U.S. Military Personnel: Risks to Privacy, Safety, and National Security" (November 2023).
[94] CIPPIC, "On the Data Trail", *supra* note 85 at 5.
[95] For example, in 2016 data broker Cambridge Analytics used data it gained from Facebook to influence the American election, in 2017 a security breach at the data broker Equifax compromised the sensitive financial information of over 150 million people, and in 2020 a New Jersey man became the third Black man in the US to be wrongfully arrested based on faulty matches using Clearview AI's facial recognition system; see Office of the Privacy Commissioner of Canada, "Data Brokers: A Look at the Canadian and American Landscape", *supra* note 85 at 3; CIPPIC, "On the Data Trail", *supra* note 85 at 7.
[96] OpenMedia, "What Canada can learn from the United States when it comes to taking on Data Brokers" (21 September 2022).
[97] *Ibid*; For example: publicly available information (s 51) and personal information collected via non-commercial activities (s 6(4));
[98] Proposed US *American Data Privacy and Protection Act* (ADPPA), the State of Vermont passed an *Act relating to data brokers*, and The California Consumer Privacy Act; *Ibid*; Byran Short, "The Absolute Bare Minimum: Privacy and the New Bill C-27" (14 September 2022).

purpose limitation, data minimization, and data-subject rights impose significant constraints on their collection, analysis, and sale of personal data.[99]

Canada must modernize its privacy regime to prevent unethical data brokerage models from being entrenched in the economy, while clarifying the obligations of organizations that pursue data brokerage as a legitimate and highly profitable revenue stream. This approach should also harmonize with US legislation to provide consistency for organizations operating in international markets.

6.1 Define "data brokers"

The CPPA must recognize the data brokerage economy to address the privacy challenges it poses. To do so, Parliament must first add the term "data broker" to the CPPA's definitions:

> **Definitions**
>
> **2 (1)** ***data broker*** means an organization with commercial activities involving the trade or analysis of personal information, and who does not collect this personal information directly from individuals.

6.2 Recognize a fiduciary duty owed by data brokers

The CPPA should impose a fiduciary duty on data brokers toward the individuals whose personal information they exploit. Such a duty would increase data brokers' legal liability, reflecting the elevated risks that the brokerage business model creates for individuals' information security, privacy, and consent.[100]

6.3 Require data brokers to provide transparency and honour a statutory opt-out

The CPPA should also require greater transparency from data brokers, to protect Canadians' privacy rights.[101] Parliament should add a subsection to section 62 imposing additional public disclosure requirements on data brokers, beyond those in subsection 62(2). To strengthen oversight and compliance, and to allow regulators to learn about the largely secretive data broker economy, these requirements should, among other things, oblige data brokers operating in Canada to register with the Office of the Privacy Commissioner.[102] Parliament should also implement a national data broker opt-out program modelled on the National Do Not Call List, with which Canadians are already familiar. Rather than depending on whether a particular data broker relies on consent, a statutory exception, publicly available information, or another legal basis for processing, the program would provide Canadians with a simple, centralized mechanism to prohibit participating data brokers from collecting, acquiring, using, disclosing, or selling their personal information, subject only to narrowly defined statutory exceptions.

---

[99] Ruschemeier, *supra* note 86 at 36.

[100] CIPPIC, "On the Data Trail", *supra* note 85 at 5; "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", 2nd reading, *House of Commons Debates*, 44-1, No 165 (7 March 2023) at 1014 (Hon Matthew Green).

[101] CIPPIC, "On the Data Trail", *supra* note 85 at 5.

[102] OpenMedia, "What Canada can learn", *supra* note 96; Short, "The Absolute Bare Minimum", *supra* note 98; OpenMedia, "Submission on C-27", *supra* note 13 at 14-16.

This regime would complement Canadians' existing rights of access, correction, and disposal under the CPPA by creating a practical mechanism for limiting participation in the data brokerage economy itself.

A centralized opt-out regime recognizes the practical realities of the data brokerage ecosystem. Individuals frequently have no direct relationship with data brokers, do not know which organizations possess their information, and cannot realistically contact hundreds of organizations individually. A statutory opt-out therefore protects privacy independently of the legal basis asserted by a particular broker, whether consent, an exception to consent, publicly available information, or another authority under the Act.

[Openness and Transparency] Data Brokers

62 (3) In addition to the requirements under subsection 62(2), data brokers must also

(a) list the parties with whom they buy and sell personal information and the products of personal information;

(b) clearly identify whether they are collecting, using or disclosing publicly available personal information according to section 51 of this Act;

(c) register as a data broker with the Office of the Privacy Commissioner; and

(d) participate in a national data broker opt-out framework that enables individuals, free of charge and through a single request, to prohibit participating data brokers from collecting, acquiring, purchasing, using, disclosing, licensing, selling, or otherwise commercially exploiting their personal information, except as expressly authorized by this Act or another Act of Parliament; and

(e) comply with any additional regulations.

Conclusion

The CPPA represents a necessary but incomplete modernization of Canada's private sector privacy regime. Bill C-27 rightly recognizes that the framework Canadians have relied on under PIPEDA, now more than two decades old, no longer answers the realities of a data-driven economy. In its current form, however, the CPPA does not deliver the protection Canadians need and deserve. It does not recognize privacy as a fundamental human right; it leaves Canadians' most sensitive information without a clear definition or a meaningful impact-assessment framework; it places anonymized data and federal political parties beyond its reach; it restructures consent and its exceptions in ways that favour commercial interests over individual rights; it offers children inadequate safeguards; and it overlooks the growing prevalence of dark patterns and the data brokerage economy.

The six recommendations advanced in this submission are directed at closing these gaps. Together, they would situate Canada's privacy framework within the international human rights tradition, extend the CPPA's scope, return individuals to the centre of consent and its exceptions, strengthen the protections owed to children, confront manipulative design, and bring data brokers within a coherent regime of accountability and transparency. Each draws on, and aligns Canada with, the leading international standards reflected in the EU's GDPR, the UK's *Data Protection Act 2018* and *Age-Appropriate Design Code*, and comparable legislation in the US

These reforms do not require Parliament to choose between privacy and innovation. As this submission has shown, the two are interdependent: meaningful privacy protection sustains the public trust on which a viable digital economy depends. Legislation that grounds responsible innovation in Canadians' right to privacy would not constrain Canada's economic growth but underwrite it.

The modernization of Canada's privacy law is an overdue opportunity. CIPPIC urges Parliament to adopt the amendments proposed in this submission so that the CPPA can offer privacy protection equal to the significance of the right it is meant to safeguard.