



# Not Fit For Purpose – Canada Deserves Much Better

Centre for Digital Rights' Report  
on Bill C-27

*Canada's Digital Charter Implementation  
Act, 2022*

First published Octobre 28, 2022  
Updated October 2, 2023\*

\* Subject to change (1) after the Minister of Innovation, Science and Industry (ISED) publishes the proposed amendments to Bill C-27 referred to in his appearance before Standing Committee on Industry and Technology (INDU) on September 26, 2023 and (2) before Centre for Digital Rights appears before INDU.

The Centre for Digital Rights (CDR) is a Canadian non-partisan, not-for-profit organization that aims to promote public awareness of digital issues related to the data-driven economy by (a) advancing the public's understanding of their rights, (b) raising policymakers' understanding of advanced technology, and (c) promoting best practices, laws and regulations that protect both the civic values and the rights of individuals in the 21st century economy, driven by the mass collection, use and disclosure of data.



## Preface to Update on October 2, 2023

This CDR Report on Bill C-27 expands on and updates the CDR Statement on Bill C-27 first published on October 28, 2022.

This updated Report:

- is intended to account for further reflection on, and important recent developments regarding, proposed “fit-for-purpose” private sector privacy legislation and artificial intelligence (AI) legislation that have occurred since the Fall of 2022 both within Canada and abroad. Specifically, this Report addresses the points summarized in Appendix H;
- is based on the version of Bill C-27 that completed Second Reading on April 24, 2023. To date, that is the current published version of the proposed legislation;
- does not and cannot consider any of the proposed amendments-in-principle that ISED Minister François-Philippe Champagne mentioned in his testimony before the INDU Committee on September 26, 2023 and that he advised would only be provided to the INDU Committee once it has started its clause-by-clause review of Bill C-27 (that is, curiously after the witnesses have presented<sup>1</sup>) including notably:
  - making privacy a fundamental right;
  - providing stricter rules on children’s privacy protection;
  - giving the Privacy Commissioner of Canada greater flexibility to reach compliance agreements;
  - defining classes of AI systems that would be treated as high impact; and
  - providing more specifics for the new Data Commissioner.

In the face of these unusual circumstances, CDR (1) objects to the government’s lack of transparency in its approach to the important work the INDU Committee must do to study Bill C-27 and (2) reserves comment on the actual legal text of these promised-but-as-yet-unpublished government amendments until they have been made public as required generally by the principles of good democratic governance and specifically by motion passed by the INDU Committee on September 28, 2023.<sup>2</sup>

1. On September 27, 2023, Professor Michael Geist called out the federal government for this secretive maneuver in his blog titled [“Why Industry Minister Champagne Broke the Bill C-27 Hearings on Privacy and AI Regulation in Only 12 Minutes.”](#) Opposition MPs on the INDU Committee from the Conservative, NDP and Bloc parties implored the Minister to table the government’s amendments at the September 26th meeting or in the very near future.
2. The text of this motion is as follows: “That pursuant to standing order 108(1) the Committee order the Minister and his department to produce the amendments discussed by the Minister in his opening remarks to the Committee on September 26, 2023, provided that these documents be deposited with the Clerk of the Committee within 5 business days and that the Minister return to speak to them.” CDR reads this motion to mean that the Minister must provide ISED’s proposed amendments to INDU by October 4, 2023.

## TABLE OF CONTENTS

	Page
Executive Summary .....	1
About the experts CDR consulted* .....	4
A. Introduction.....	5
B. Recommendations to fix Bill C-27's problems and make it fit for purpose .....	7
1. Make Bill C-27 fit for addressing current privacy challenges and consistent with contemporary global privacy standards .....	7
2. Frame the purposes of Bill C-27 properly .....	9
2.1 Recognize privacy as a fundamental human right. ....	9
2.2 Change the proposed legislation's name from " <i>Consumer Privacy Protection Act</i> " (CPPA) to " <i>Canada Personal Information Protection Act</i> " (CPIPA) or " <i>Canada Privacy Protection Act</i> " (CPPA).....	10
2.3 Consult with Indigenous Peoples in modernizing Canadian privacy legislation including PIPEDA. ....	10
3. Address the privacy risks to democracy .....	10
3.1 Expressly extend the CPPA to cover Canada's federal political parties (FPPs). ...	11
4. Recognize the serious privacy risks to groups as well as to individuals .....	12
4.1 Extend privacy protection to mitigate risks to groups. ....	12
4.2 Define “sensitive information” in keeping with the general principle of sensitivity set forth in section 12 of Quebec's Law 25 and the special categories of sensitive personal information (PI) enumerated in GDPR Article 9 (to ensure "adequacy") but on a non-exhaustive basis and with the addition of location-tracking information. ....	12
4.3 Protect minors with special, enhanced privacy requirements.....	13
4.4 Clearly specify certain no-go zones as always being inappropriate purposes for collecting, using and/or disclosing an individual's PI.....	14
5. Fix the consent provisions. ....	14
5.1 Strengthen valid consent in section 15 of the CPPA by restoring the "understanding" requirement in section 6.1 of PIPEDA.....	14
5.2 Adopt a "legitimate interests" rule that clearly ranks the individual's interests and fundamental rights above the commercial interests of the organization in any assessment of the impact of relying on the rule.....	15
5.3 Eliminate implied consent as an alternative to the express consent basis for permitted collection, use, or disclosure of PI.....	15

5.4 Require separate, opt-in consent on digital media for collection, use or disclosure of personal information for purposes beyond what is necessary to provide a product or service. ....16

5.5 Specify that the appropriate standard for determining the general impression to the average individual when ascertaining whether their consent has been obtained "deceptively" (and so is invalid) is the credulous and inexperienced person as opposed to the reasonable person. ....16

5.6 To address the concerns with the consent provisions raised in recommendations 5.1 through 5.5 above, sections 15, 16 and 18 of the CPPA should be revised.....17

6. Use all the tools in the "privacy and consumer protection toolbox" to promote accountability .....23

6.1 Require organizations to conduct privacy impact assessments (PIAs) in advance of product or service development - particularly where invasive technologies and business models are being applied, where minors are involved, where sensitive PI is being collected, used, or disclosed, and when the processing is likely to result in a high risk to an individual's rights and freedoms.....24

6.2 Expressly require organizations to protect (i) privacy by "default" to align with Quebec's Law 25, section 9.1 and (ii) personal data by "design and default" to align with the GDPR, Article 25 (to help ensure "adequacy"). ....24

6.3 Promote the development of data stewardship models.....24

6.4 Strengthen security safeguards. ....25

6.5 Like Quebec's Law 25, the CPPA should have a separate section for cross border data flows requiring that organizations in Canada that export PI to a foreign jurisdiction for processing must first conduct a PIA to establish that the PI will receive an equivalent level of protection as in Canada.....25

6.6 Adopt a more comprehensive regime governing third party data processors/service providers. ....26

6.7 Clearly impose transparency and accountability obligations on data brokers.....26

7. Strengthen individuals' control over their PI .....27

7.1 Provide for a more comprehensive right to PI "mobility" (aka "portability").....27

7.2 Limit the exceptions to the right to "disposal" of PI (aka a right to "deletion"/"erasure"/"be forgotten") and provide for a right to disposal with respect to search engines' indexing of individuals' PI in specified circumstances.....28

7.3 Strengthen information and access. ....28

7.4 Prohibit, subject to specific and narrow exceptions, organizations from using ADS/AI to collect, use or disclose an individual's PI as the basis for decisions about them to align with GDPR, Article 22 (to help ensure "adequacy"). ....28

7.5 Give individuals the rights to contest and object to ADS/AI affecting them, not just a right to "algorithmic transparency". ....29

7.6	Strengthen the private right of action (PRA).....	30
7.7	Adjust the CPPA's proposed regime for non-identifiable information (i) to make clear that organizations must apply appropriate processes to de-identify information and protect any such information and (ii) to provide that anonymized information complies with standards set out in regulations, to align with Quebec's Law 25.....	31
8.	Give the Privacy Commissioner more teeth and bite.....	31
8.1	Scrap the proposed Personal Information and Data Protection Tribunal. ....	31
8.2	Provide for more flexible enforcement. ....	32
8.3	Equip the Privacy Commissioner with the power to seek the imposition of administrative monetary penalties (AMPs) in a manner similar to the powers of the Commissioner of Competition under the <i>Competition Act</i> .....	32
8.4	Empower the Privacy Commissioner to issue "enforcement notices" and expand the sections for which the Privacy Commissioner can recommend penalties to include violations of the following: 12(1) (Appropriate purposes); 55 (3) (Disposal at individual's request: Reasons for refusal); 73 (Complaints and requests for information); 75 (Prohibition on re-identification); and 97 (Audits).....	33
8.5	Strengthen the inter-agency collaboration and information-sharing provisions between the Privacy Commissioner, the Commissioner of Competition, and the CRTC. ....	33
8.6	Strengthen the whistleblowing regime.....	33
8.7	Implement a self-reporting program for organizations.....	34
9.	The <i>Artificial Intelligence and Data Act</i> (AIDA) is foundationally flawed, needs proper consultation, and should be sent back to the drawing board (but don't leave it to ISED alone)....	34
9.1	AIDA is improper and incomplete.....	34
9.2	AIDA inappropriately focuses excessively on risks of harms to individuals to the exclusion of collective harms.....	35
9.3	AIDA possesses contradictory language and fragile enforcement powers.....	36
9.4	AIDA inappropriately focuses on an overly narrow range of algorithmic techniques. ....	36
9.5	Go back to the drawing board on AIDA, but don't leave it to ISED alone.....	36
C.	Summary and Conclusion.....	39
Appendix A	Other recommendations to strengthen Bill C-27.....	41
10.1	Hold directors and officers personally liable. ....	41
10.2	Equip the Privacy Commissioner with the power to seek disgorgement of the organization's profits accruing from its unlawful activity under the CPPA. ....	41
Appendix B	Recommendations for further study .....	42
11.1	Develop and implement a new and robust home-grown "control by design" governance framework to reset the old and failing "privacy by design and default"	

protections that were first developed in Canada in the 1990's, more recently gained prominence in privacy law reform in many jurisdictions (including Quebec and throughout the EU), but alone are now not fit for purpose and must be modernized. ....42

11.2 Establish a fiduciary responsibility that imposes duties of loyalty and care on organizations that collect and use PI from individuals in circumstances of significant power and information imbalances or where individuals lack the ability to ensure compliance. 43

11.3 Provide the Office of the Privacy Commissioner with sufficient funding for it to properly fulfill its mandate.....45

11.4 Consider establishing a complaint funding mechanism to help finance legal proceedings brought by individual or group complainants and/or public interest organizations seeking remedies against organizations for alleged contraventions of the CPPA. ....47

11.5 Protect the complainant's confidentiality and anonymity throughout the complaint process, including judicial reviews and appeals .....48

Appendix C Summary of over 40 recommendations (i) to fix Bill C-27's problems and make it fit for purpose, (ii) to strengthen Bill C-27, and (iii) for further study.....49

Appendix D Busting the myth that stricter privacy regulation stifles innovation .....53

Appendix E CDR's critique of the CMA's Privacy Reports .....56

Appendix F CDR's Critique of the ISED's Companion Document for AIDA.....67

Appendix G CDR's critique of the federal government's amendment to the *Canada Elections Act* as part of Bill C-47 (the 2023 Budget legislation) purporting to implement a "national, uniform, exclusive and complete regime" for the FPPs' protection of Canadians' privacy .....72

Appendix H Summary of new points in CDR's Report on C-27 dated October 2, 2023 updating CDR's C-27 Statement on C-27 dated October 28, 2022 .....79

Appendix I Annotated bibliography .....81

## Executive Summary

There is widespread agreement that the *Personal Information Protection and Electronic Documents Act (PIPEDA)* is past its expiry and in urgent need of updating. Bill C-27, *Canada's Digital Charter Implementation Act, 2022*, attempts to tackle private sector privacy regulation by introducing three proposed laws: the *Consumer Privacy Protection Act (CPPA)*, the *Personal Information and Data Protection Tribunal Act (PIDPTA)* and the *Artificial Intelligence and Data Act (AIDA)*. Regrettably, as presented, Bill C-27 misses the opportunity to produce a path-breaking statute that addresses the enormous risks and asymmetries posed by today's surveillance business model.

Twenty years ago, Canada was judged by the European Commission to have provided an "adequate level of protection" at least for businesses covered by PIPEDA, thus allowing personal data to flow to Canada without any further safeguards being necessary. The bar has now changed as a result of European court judgements as well as a landmark and innovative 2018 European law, the General Data Protection Regulation (**GDPR**). It is critically important for Canadian businesses that the adequacy judgment is not rescinded. The judgement about adequacy is a formal one, and may involve decisions of several European institutions and courts. Canada should not assume that, just because it enjoyed this status with PIPEDA, this is bound to continue.

Canadians also care about their privacy. In a recent [survey](#)<sup>3</sup>, 93% of Canadians expressed concerns about the protection of their privacy. Fewer Canadians believe that businesses are respecting their privacy rights, and only 1 in 10 Canadians trust social media companies to protect their personal information.

In consultation with some of Canada's leading privacy experts and thought leaders, the Centre for Digital Rights (**CDR**) has prepared this Report on Bill C-27, recommending to **make Bill C-27 fit for addressing Canada's current privacy challenges and consistent with contemporary global privacy standards**. This Report aims to assist in the vital task of remediating the deficiencies of Bill C-27, by drawing on Canada's history of privacy innovation and examples from leading jurisdictions elsewhere. It offers specific recommendations for making the proposed CPPA fit for current and future challenges and highlights the concerns of rushing unnecessary (PIDPTA) and inadequate (AIDA) legislation.

CDR's key recommendations for fixing Bill C-27 include:

- The CPPA should **recognize privacy as a fundamental human right** that is inextricably linked to other fundamental rights and freedoms. As a human right, it is not appropriate to "balance" privacy against commercial interests, though any loss of privacy would be balanced against other fundamental rights, such as the right to freedom of expression.
- The CPPA should address the **privacy risks to democracy** and extend the CPPA to cover Canada's federal political parties (**FPPs**). It is the height of cynicism and hypocrisy

---

<sup>3</sup> Office of the Privacy Commissioner of Canada, *2022-23 Survey of Canadians on Privacy-Related Issues*, March 2023 [https://www.priv.gc.ca/en/opc-actions-and-decisions/research/explore-privacy-research/2023/por\\_ca\\_2022-23/](https://www.priv.gc.ca/en/opc-actions-and-decisions/research/explore-privacy-research/2023/por_ca_2022-23/)

for the FPPs to keep ignoring recommendations from privacy commissioners in Canada and abroad, the House of Commons Standing Committee on Access to Information, Privacy and Ethics (the **ETHI Committee**), privacy and data governance experts, advocates, and public opinion polls to expressly include FPPs under federal private sector privacy law, and then ask all other organizations to follow rules that the FPPs refuse to follow themselves. The federal government's recent amendment of the *Canada Elections Act* purporting to provide a uniform and exclusive approach to how the FPPs protect Canadians' privacy is both hypocritical and a violation of the *Constitution of Canada* ("**Canada's Constitution**") and the *Canadian Charter of Rights and Freedoms* (the "**Charter**"). In separate prepared remarks to the Senate Standing Committee on Legal and Constitutional Affairs on May 3, 2023 (see Appendix G for details), this amendment (when it was just a proposal) was described by both the Privacy Commissioner of Canada and Canada's Chief Electoral Officer as inadequate to protect Canadians' personal information and falling short of their recommendations for meaningful privacy obligations on the FPPs.

- The federal government should **consult meaningfully with Indigenous Peoples and recognize Indigenous data sovereignty**. Its failure to do so is inconsistent with the federal government's obligation to implement the *United Nations Declaration on the Rights of Indigenous Peoples*. It is unacceptable and inexcusable, especially in light of the well-established and well-known First Nations Principles of OCAP®. Indigenous voices must not be left out if the federal government is serious about building a foundation of trust in the digital world in Canada.
- Privacy protection should be extended to **recognize the privacy risks to groups as well as to individuals**. The CPPA should extend protection to groups that are sufficiently defined such as households and children in a classroom. "Sensitive information" should be appropriately defined in the statute and minors should be better protected with special, enhanced privacy requirements.
- The CPPA requires a **fix to the consent provisions**, since the CPPA has eliminated important consent language from PIPEDA and omitted the guardrails necessary to ensure adequate privacy protections that clearly rank the individual's interests and fundamental rights above the commercial interests of the organization. Express, opt-in consent should be sought on digital media for the collection, use or disclosure of personal information for purposes beyond what is necessary to provide a product or service. This form of consent should be unbundled from the terms of use, and not made a condition of providing the product or service. Sections 15 and 18 (re: legitimate interest) of the CPPA should be rewritten.
- The CPPA should **use all the tools in the "privacy and consumer protection toolbox" to promote accountability**. This includes requiring privacy impact assessments (**PIAs**) in advance of the use of invasive technologies or high-risk processing, stipulating privacy-by-default requirements, promoting the development of data stewardship models,



additional requirements surrounding cross-border data flows, and a more comprehensive regime governing third party data processors/service providers.

- The CPPA should **strengthen individuals' control over their personal information (PI)**, for example, by providing a more comprehensive right to data mobility (or portability) and limiting the exceptions to the right to disposal of PI.
- The CPPA should **give the Office of the Privacy Commissioner more teeth and bite**. The CPPA should equip the Privacy Commissioner with more flexible enforcement approaches as well as the power to impose administrative monetary penalties. The PIDPTA should be scrapped. No justification (privacy law innovation or otherwise) has been given for such a tribunal. Its assigned role and composition raise serious concerns (including unnecessary complexity, delay and uncertainty for both individuals and organizations in the resolution of a complaint). Further, there is no privacy law regime in the world (including the modern and progressive regime in the EU, as well as the regimes in California, Utah, Colorado, Virginia and Connecticut, and the proposed *American Data Privacy and Protection Act*) that has established a tribunal like the Tribunal being proposed under the PIDPTA. Nor is such a tribunal proposed in the Australian Government's February 16, 2023 Privacy Act Review Report 2022 .
- AIDA should be sent back to the drawing board, but not to ISED alone. It is improper and incomplete, and inappropriately focuses excessively on risks of harms to "individuals" rather than on risks of harms to "groups and communities" (also known as "collective" harms).

Canada has the opportunity to learn from the best of current global data protection standards, to fashion a path-breaking statute and to truly "modernize" its legislation (including by developing and implementing a new and robust *control by design* governance framework). Regrettably, Bill C-27 is not consistent with contemporary global standards. It falls short in addressing the serious privacy challenges that have emerged since PIPEDA was enacted. Most importantly, it fails to address the reality that dominant data-driven enterprises have shifted away from a service-oriented business model towards one that relies on monetizing PI through the mass surveillance of individuals and groups.

### **About the experts CDR consulted\***

*\*The unpaid, voluntary, and significant contribution of each expert to this Report is gratefully acknowledged.*

#### **Dr. Colin Bennett**

Colin Bennett is Professor Emeritus of Political Science at the University of Victoria, British Columbia and Associate Fellow at the Centre for Global Studies. For over thirty years, his research has focused on the impact of surveillance technologies, and on the comparative analysis of privacy protection governance at domestic and international levels. In addition to numerous scholarly and newspaper articles, he has published seven books on these subjects, including *The Governance of Privacy* (MIT Press, 2006), as well as policy reports for national and international organizations, including the Privacy Commissioner of Canada, the European Commission, the Council of Europe and the UK Information Commissioner. He is currently researching the capture and use of personal data on voters by political parties in Western democracies. For more information, please see his website: <https://www.colinbennett.ca/>

#### **Dr. Andrew Clement**

Dr. Andrew Clement is Professor Emeritus in the Faculty of Information at the University of Toronto, where he coordinates the Information Policy Research Program and co-founded the Identity Privacy and Security Institute. With a Ph.D. in computer science, he has had long-standing research and teaching interests in the social implications of information/communication technologies, participatory design, surveillance and privacy. His recent projects have focussed on advancing transparency and accountability of internet-based surveillance.

#### **Dr. Teresa Scassa**

Dr. Teresa Scassa is the Canada Research Chair in Information Law and Policy at the University of Ottawa, Faculty of Law. She is a member of the Canadian Advisory Council on Artificial Intelligence, and a past member of the External Advisory Committee of the Office of the Privacy Commissioner of Canada. She was appointed the first-ever scholar-in-residence at the Office of the Information and Privacy Commissioner of Ontario serving from September 2022 to June 2023. She has written widely in the areas of privacy, technology (including artificial intelligence), and intellectual property law. For more information, please visit her blog at: <http://www.teresascassa.ca>

## A. Introduction

There is widespread agreement that the *Personal Information Protection and Electronic Documents Act* (**PIPEDA**) is past its expiry and in urgent need of updating. In this regard, the federal government's proposed *Digital Charter Implementation Act, 2022* (**Bill C-27**) is a welcome development. Regrettably, however, Bill C-27, as presented, misses the opportunity to produce a path-breaking statute that addresses the enormous risks and asymmetries posed by today's surveillance business model.

Bill C-27 attempts to tackle private sector privacy regulation by introducing three proposed laws: the *Consumer Privacy Protection Act* (**CPPA**), the *Personal Information and Data Protection Tribunal Act* (**PIDPTA**) and the *Artificial Intelligence and Data Act* (**AIDA**). Bill C-27 fixes some of the more glaring shortcomings of PIPEDA's "light touch" regulatory regime, notably by granting Canada's Privacy Commissioner the power to make binding orders and to recommend the imposition of administrative monetary penalties (**AMPs**) in certain circumstances. However, at the same time, it weakens certain data protection measures.

This lack of consistency led Canada's former Privacy Commissioner Daniel Therrien to characterize Bill C-27's predecessor, former Bill C-11, as a "step back overall for privacy".<sup>4</sup> Unfortunately, the current bill does no better overall. While Canada's current Privacy Commissioner Philippe Dufresne states that Bill C-27 is "in many ways an improvement over both the PIPEDA and the former Bill C-11" and thus a "step in the right direction", he is quick to emphasize in the Submission of the OPC on Bill C-27 dated April 2023 that Bill C-27 "can and must be further improved".<sup>5</sup> Bill C-27 falls short in addressing the serious privacy challenges that have emerged since PIPEDA was enacted. Most importantly, it fails to address the reality that dominant data-driven enterprises have shifted away from a service-oriented business model towards one that relies on monetizing personal information (**PI**) through the mass surveillance of individuals and groups. This lightly regulated model has proven enormously lucrative, producing a new generation of tech giants of unprecedented size and reach and exacerbating the power asymmetries these organizations already enjoyed vis-a-vis data subjects (both individuals and groups).

The proposed bill also does not align with contemporary global standards or the current reality of PI flows. Although PIPEDA passed an "adequacy test" some twenty years ago, under the EU's *Data Protection Directive*, Parliament should not presume that Bill C-27 will meet the heightened bar of "essential equivalence" under the EU's more stringent *General Data Protection Regulation* (**GDPR**). It is critically important for both Canadian businesses and Canadians that "adequacy" be maintained. Canadians also care about their privacy. In a recent survey, 93% of Canadians expressed concerns about the protection of their privacy. Fewer Canadians believe that businesses

---

<sup>4</sup> Office of the Privacy Commissioner of Canada, Submission on Bill C-11, the *Digital Charter Implementation Act*, 2020, May 2021, online:

[https://www.priv.gc.ca/en/opc-actions-and-decisions/submissions-to-consultations/sub\\_ethi\\_c11\\_2105/](https://www.priv.gc.ca/en/opc-actions-and-decisions/submissions-to-consultations/sub_ethi_c11_2105/)

<sup>5</sup> 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, online: [https://priv.gc.ca/en/opc-actions-and-decisions/submissions-to-consultations/sub\\_indu\\_c27\\_2304/](https://priv.gc.ca/en/opc-actions-and-decisions/submissions-to-consultations/sub_indu_c27_2304/)

are respecting their privacy rights, and only 1 in 10 Canadians trust social media companies to protect their personal information.<sup>6</sup>

It is therefore increasingly urgent for data protection legislators to remediate these deficiencies and to provide Canadians with an effective means to assert their privacy rights and to hold organizations accountable. This Report aims to assist in this vital task. By drawing on Canada's history of privacy innovation and examples from leading jurisdictions elsewhere, it offers specific recommendations (including, for further study, one to implement a new and robust *control by design* governance framework) for making the proposed CPPA fit for current and future challenges and highlights the concerns of rushing unnecessary (PIDPTA) and inadequate (AIDA) legislation.

---

<sup>6</sup> Office of the Privacy Commissioner of Canada, *2022-23 Survey of Canadians on Privacy-Related Issues*, March 2023 [https://www.priv.gc.ca/en/opc-actions-and-decisions/research/explore-privacy-research/2023/por\\_ca\\_2022-23/](https://www.priv.gc.ca/en/opc-actions-and-decisions/research/explore-privacy-research/2023/por_ca_2022-23/)

## B. Recommendations to fix Bill C-27's problems and make it fit for purpose

### 1. Make Bill C-27 fit for addressing current privacy challenges and consistent with contemporary global privacy standards

*Bill C-27 should be more closely aligned with the GDPR in order to ensure that Canada is recognized as a country with adequate personal data protection rules.*

Canada used to be seen as a pioneer and known for its forward-looking thinking about how to protect privacy against the worst abuses of digital technologies. Regrettably, Bill C-27 is not consistent with contemporary global standards. Indeed, ideas and policy tools, noted below, once pioneered in Canada and exported to other countries do not appear in Bill C-27. The government has missed a huge opportunity to produce a path-breaking statute, fit for the purpose of addressing the enormous risks posed by surveillance capitalism and the business models that it inspires and supports.

Personal data flows globally, but to read this statute one would not know it. Unlike other contemporary privacy statutes, there is no dedicated section which clarifies the rules for the transfer of personal data outside of Canada (Chapter 5 of the GDPR contains seven separate articles on this question). Quebec's Law 25 (formerly Bill 64) also addresses these issues in more detail than Bill C-27. As noted below, this is a major gap in the proposed federal legislation that needs to be fixed for both Canadians and Canadian businesses. It is also a gap that could threaten an assessment of adequacy under European law.

Like it or not, the GDPR is widely seen as the *de facto* global standard for international data protection. There is a narrative common in business circles that the GDPR is overly prescriptive, rule-based and top-down.<sup>7</sup> That narrative supposedly contrasts this European bureaucratic approach with the more flexible "principles-based" approaches upon which PIPEDA, and now Bill C-27, are based. This dichotomy is false. The GDPR maintains all the flexibility necessary for businesses to process personal data for their legitimate needs. The claim that it, and European law generally, stifles innovation is without evidence. It's a myth (see summary of research in Appendix D). We should reject the narrative that this "flexible", "made-in-Canada" approach is more fit-for-purpose than the more "bureaucratic" approaches in Europe. It is not.

Twenty years ago, Canada was judged by the European Commission to have provided an "adequate level of protection" at least for businesses covered by PIPEDA, thus allowing personal data to flow to Canada without any further safeguards being necessary. The bar

---

<sup>7</sup> The U.K. government recently used this narrative with respect to its *Data Protection and Digital Information (No. 2) Bill* (the "DPDI"). That said, the DPDI is a mostly unchanged version of the original Bill announced in July 2022 that followed a co-design process with industry, business, privacy and consumer groups. While much discussion has ensued over the DPDI and whether it will be deemed "adequate" to the GDPR, the reality is that the DPDI lacks substantial deviations from the existing GDPR framework and is simply "GDPR-lite". While there has been much showmanship surrounding the DPDI, the DPDI clearly signals the U.K. government is aware of the risk of losing adequacy status with the GDPR if it sways too far from the existing GDPR framework, a move that would be highly disruptive and detrimental to many U.K. businesses.

has now changed as a result of European court judgements and the GDPR. "Essential equivalence" to European data protection law is now the test of adequacy – and a higher threshold than when PIPEDA was deemed adequate 20 years ago. It is critically important for Canadian business that the adequacy judgment is not rescinded. Over and above any economic advantages, adequacy is of symbolic importance, positioning Canada as a place where privacy rights continue to be respected. Furthermore, global businesses are already claiming that their operations are GDPR compliant/consistent – including many Canadian businesses. So why should there be any unnecessary divergences between the GDPR and Bill C-27? We could end up with the situation where businesses are providing more rights to Europeans and greater protection to European data, than they do for Canadians. Consistency with the GDPR is, therefore, important for the global interoperability of data protection standards, and the competitiveness of Canadian companies.

CDR understands that Canadian officials may have been given private assurances that Bill C-27 meets this bar of "essential equivalence". Canada should not be so confident. Noted in this Report are several areas of Bill C-27 that are significantly weaker than the GDPR, and provide significantly lower privacy rights for Canadians, in comparison with Europeans. Many of CDR's recommendations in this Report on Bill C-27 would significantly enhance the likelihood of Canada achieving essential equivalence. The judgement about essential equivalence, under Article 45 of the GDPR is a formal one, involving the Commission, the European Data Protection Board, representatives of EU countries, and potentially the European Parliament. Decisions about essential equivalence may also be challenged in the European Courts. Canada should not assume that, just because we enjoyed this status with PIPEDA, this is bound to continue. As discussed in more detail below, the essential equivalence of Bill C-27 against these European standards is highly questionable.

In the OPC's Submission on Bill C-27 to the *House of Commons Standing Committee on Industry and Technology ("INDU")* (May 2023), the Federal Privacy Commissioner, Philippe Dufresne, referred to Bill C-27 as "a step in the right direction" but stated that the Bill "can and must be further improved". The OPC's Submission contains 15 Key Recommendations with suggested amendments for Bill C-27, as well as an appendix, which lists additional ways to further enhance Bill C-27, based on the OPC's previous recommendations on the former Bill C-11. The OPC's recommendations include: to recognize privacy as a fundamental right, to protect children's privacy, to expand the list of violations qualifying for AMPs, to strengthen the framework for de-identified and anonymized information, to require organizations to explain on request all predictions, decisions and profiling using automated decision systems, to conduct PIAs for high risk initiatives, to expand the OPC's ability to coordinate with other bodies, to conduct PIAs for high-risk initiatives, to limit the exception to the right to disposal regarding an organization's record retention schedule, and to provide greater flexibility in the use of voluntary compliance agreements. These recommendations align closely with those submitted in this Report.

## 2. **Frame the purposes of Bill C-27 properly**

*Unlike the private sector privacy laws of many other countries around the world, Bill C-27 fails to enshrine privacy as a fundamental human right. It is wholly inappropriate to balance a loss of privacy with the potential for commercial benefits. CDR recommends to:*

### 2.1 **Recognize privacy as a fundamental human right.**

The CPPA should expressly recognize privacy as a fundamental human right that is inextricably linked to other fundamental rights and freedoms including the rights to life and liberty (personal autonomy and self-determination), freedom of thought and expression, freedom from discrimination, and freedom from unjustified intrusion or surveillance. Such recognition should be made in both a new preamble to the CPPA itself (note that the current preamble, which arguably only applies to Bill C-27 overall, does not contain such recognition) and section 5 (Purpose) of the CPPA in order to provide clear guidance to those interpreting the CPPA. The addition of a reference to privacy as a fundamental human right in the preamble of the CPPA alone may be insufficient; to avoid any doubt, specific inclusion is needed in the body of the CPPA to give unambiguous legal effect to Parliament's intention that privacy be recognized as a fundamental human right. As in the GDPR, the privacy rights of individuals should prevail over commercial interests and not be "balanced" against them. As a fundamental human right, it is not appropriate to "balance" privacy against commercial interests or provide that any loss of privacy should be proportionate to the commercial benefits. However, any loss of privacy must be balanced against other fundamental rights, such as the right to freedom of expression. A fundamental right to privacy addresses the right to control an individual's PI and its processing with particular application in the automated decision system (ADS)/artificial intelligence (AI) context, where risks to fundamental rights (such as the right to be free from discrimination and arbitrary decisions) are heightened. The Office of the Privacy Commissioner of Canada (OPC) published an opinion by Addario Law Group LLP on March 31, 2022 indicating that a human rights-based approach to data protection is constitutional.

The Federal Court of Canada's April 13, 2023 decision, [Privacy Commissioner of Canada v. Facebook, Inc., 2023 FC 533 \(Facebook Application Decision\)](#) also exemplifies the need for a human rights framework in privacy legislation. The decision refers to PIPEDA's balancing clause, speaking to the need to balance individual and organizational interests. However, as instances such as the Cambridge Analytica scandal demonstrate, personal information unlawfully used can lead to profiling and micro-targeting with misinformation for political purposes. Privacy should not be "traded off" against organizations' desires and interests. It should be recognized as a fundamental human right, allowing an individual to have more control over their private life and personal information. Any balancing should be undertaken from the viewpoint of privacy as a fundamental human right.

2.2 **Change the proposed legislation's name from "*Consumer Privacy Protection Act*" (CPPA) to "*Canada Personal Information Protection Act*" (CPIPA) or "*Canada Privacy Protection Act*" (CPPA).**

Replacing "Consumer" with "Canada" better reflects the intended scope of the legislation – namely, to protect, in the context of the commercial activities of Canada's private sector organizations, the PI of all Canadians, not just those who are acting as "consumers".

2.3 **Consult with Indigenous Peoples in modernizing Canadian privacy legislation including PIPEDA.**

The federal government's failure to consult with Indigenous Peoples regarding modernizing PIPEDA has been called out by the Citizen Lab at the University of Toronto in a critical analysis of Bill C-27 entitled *Minding Your Business* published on November 22, 2022 (in particular, see pages 37-38 and 54). The same point is made by University of Toronto Professors Lisa Austin and John Borrows in their December 6, 2022 commentary entitled *The Digital Charter Implementation Act Ignores Indigenous Data Sovereignty*. This failure is inconsistent with the federal government's obligation to implement the *United Nations Declaration on the Rights of Indigenous Peoples (UNDRIP)*; and it is unacceptable and inexcusable, especially in light of the well-established and well-known First Nations Principles of OCAP® (i.e., ownership, control, access, and possession) first enunciated in 1998. These principles assert that First Nations have control over data collection processes, and that they own and control how this information can be used.

Simply put, Indigenous voices must not be left out if the federal government is serious about building a foundation of trust in the digital world in Canada. Accordingly, at a minimum, the federal government should now start consulting with the Assembly of First Nations (AFN), the expert technical organization, the First Nations Information Governance Centre (FNIGC), and most importantly, the rights holders themselves. Moreover, the federal government must provide such Indigenous stakeholders with appropriate timelines and capacity supports to enable them to participate meaningfully in such consultations. CDR understands, having reached out to both the AFN and FNIGC, that the FNIGC has published several resources pertinent to Canadian privacy law modernization including an August 2022 discussion paper entitled *Exploration of the Impact of Canada's Information Management Regime on First Nations Data Sovereignty* and more recently a March 2023 paper entitled *PIPEDA and First Nations: Application and Reform*.

3. **Address the privacy risks to democracy**

*Recent scandals have demonstrated unequivocally how the processing of PI by political parties and other actors can have damaging consequences for democratic institutions. It is, therefore,*



completely unjustifiable that Canada's federal political parties (FPPs) are not expressly subject to the CPPA.

### 3.1 Expressly extend the CPPA to cover Canada's federal political parties (FPPs).

It is the height of cynicism and hypocrisy for the FPPs to keep ignoring recommendations from privacy commissioners in Canada and abroad, Canada's Chief Electoral Officer, the ETHI Committee, privacy and data governance experts, advocates, and public opinion polls, to expressly include FPPs under federal private sector privacy law, and then ask all other organizations to follow rules that the FPPs refuse to follow themselves. It is unlikely that this purported carve-out would survive an "adequacy" test under the GDPR particularly for a Canadian living in the EU because it would violate the prohibition (with only limited exceptions) on "processing of personal data revealing... political opinions" in GDPR Art 9(1).

This express extension can be accomplished by (1) adding to subsection 6(1) of the CPPA, a new paragraph (c) that reads "(c) is collected, used or disclosed by a federal political party, a candidate, an electoral district association, or a nomination contestant in connection with electoral activities"; and (2) adding appropriate definitions of "federal political party", "candidate", "electoral district association" and "nomination contestant" to have the meanings as under the *Canada Elections Act*, and of "electoral activities" to encompass any activities related to promoting a federal political party at any time – that is, whether during a formal election period or otherwise.

It is worth noting that in British Columbia, the Office of the Information and Privacy Commissioner has recently found that the FPPs are subject to British Columbia's *Personal Information Protection Act*. In sum, the CPPA can and should apply to the FPPs. Extending its application to them would be a straightforward step that can be accomplished right now. Furthermore, the Australian Government, in its Attorney-General's Department's Privacy Act Review Report 2022 published on February 16, 2023, has recommended that registered political parties in Australia be covered by the same private sector privacy law that governs all private sector organizations.

The federal government's amendment to the *Canada Elections Act* that received Royal Assent on June 22, 2023 purportedly to provide for a national, uniform, exclusive and complete regime in respect of the FPPs' collection, use and disclosure of Canadians' personal information in a manner that purports to override all provincial privacy laws is not only hypocritical, it would be a violation of Canada's Constitution and the Charter, and it should outrage Canadians for the reasons summarized in Appendix G.

#### 4. **Recognize the serious privacy risks to groups as well as to individuals**

*There are serious privacy risks whenever an individual is classified, sorted and profiled according to their PI. These risks may be heightened when the data subject is a group. Privacy law reform should, therefore, recognize and address the risks to groups, as well as to individuals. Several amendments will achieve this goal.*

##### 4.1 **Extend privacy protection to mitigate risks to groups.**

The CPPA should, for all Canadians, extend protection to information that would be considered personal to groups that are sufficiently defined such as households and children in a classroom. Like individuals, groups can also be tracked, profiled, sorted, and targeted and this can have an adverse impact both on groups and individuals within those groups.

##### 4.2 **Define “sensitive information” in keeping with the general principle of sensitivity set forth in section 12 of Quebec's Law 25 and the special categories of sensitive personal information (PI) enumerated in GDPR Article 9 (to ensure "adequacy") but on a non-exhaustive basis and with the addition of location-tracking information.**

At the moment, the definition of sensitive categories of personal information is left open and the words "sensitive" and "sensitivity" are used throughout Bill C-27 without definition (with the exception of minors). Thus, the definition is left to the organization with the obvious risk that some sensitive data will not be regarded as such, and that interpretations will vary.

So as to provide greater certainty for Canadians and Canadian businesses, and to align with both Quebec's Law 25 and the GDPR, Bill C-27 should define "sensitive information" first by establishing a general principle of sensitivity followed by an explicitly open-ended list of examples (including location-tracking information and the special categories of sensitive personal data enumerated in the GDPR, Article 9 – namely, PI revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetics, biometrics, health, sex life, or sexual orientation).

Therefore, along the lines suggested by the OPC in its May 2021 submission regarding former Bill C-11, such a definition might read:

**"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 and includes: (a) information revealing racial or ethnic origin, gender identity, sex life, sexual orientation, political opinions, group affiliation, or religious or philosophical beliefs; (b) genetic information; (c) biometric information;

(d) financial information; (e) health information; and (f) location-tracking information.

#### 4.3 **Protect minors with special, enhanced privacy requirements.**

There is a broad consensus that the internet was not designed with minors in mind. That said, the CPPA only gestures at minors' needs for privacy protections by calling their PI "sensitive" and contains no measures that curtail the prevailing online surveillance and behavioural manipulation practices of businesses or even reduce the incentive for businesses to track minors. The CPPA should advance specific protections for children and youth such as defining rules for age-appropriate consent, establishing privacy-respectful processes and mechanisms for age verification, and providing for a comprehensive code of practice for organizations collecting, using or disclosing children's PI (such as the UK's September 2020 *Children's Code* in force since 2021 and the September 2022 *California Age-Appropriate Design Code Act* that comes into force on July 1, 2024). Notably, there is a proliferation of such minors' protection measures globally including in Ireland, the Netherlands, and Argentina. In the US, many laws aiming to enhance protections for children's PI or minors' use of social media have been adopted or proposed, including in Utah, Connecticut, Ohio, Arkansas, Oregon, Illinois, Maryland, Nevada, New Mexico, Texas, California, Florida, Iowa, Louisiana, Maryland, Minnesota, South Carolina, and New Jersey.

Here in Canada, in April 2023, the BC OIPC published a Report indicating it is in the early stages of developing a code to clarify organizations' obligations under BC privacy law regarding minor's PI. Quebec's Commission d'accès à l'information (CAI), in its [Report](#) to the Minister responsible for Access to Information and Privacy Protection of Personal Information, also suggested that Law 25 be strengthened to enhance privacy protections for children.<sup>8</sup>

Any minor's code advanced under the CPPA should take into account the best interest of the minor as a primary concern and should require, among other things, (1) the conduct of privacy impact assessments (**PIAs**) to mitigate the risk to minors that arise from the collection, use, or disclosure of their PI, (2) using high privacy settings by default, (3) age-appropriate parental controls, and (4) age-appropriate tools to report concerns. Consistent with emerging international norms, such a code should also prohibit outright organizations from collecting a minor's precise location, using nudge techniques (even if they don't qualify as deceptive dark patterns), and sharing minors' data with third parties unless there is a compelling reason to do so and it is in the best interest of the minor.

---

<sup>8</sup> *Ensuring a better protection for young people's personal information in the digital age*; Commission d'accès à l'information, August 2022.

4.4 **Clearly specify certain no-go zones as always being inappropriate purposes for collecting, using and/or disclosing an individual's PI.**

These inappropriate purposes and prohibitions should include (1) psychographic micro-profiling and micro-targeting for purposes of persuasion or influencing behaviour and (2) capturing biometric data without express consent (e.g., facial image scraping from websites, platforms and other locations on the Internet).

5. **Fix the consent provisions.**

*The requirements for express and implied consent, and their relationship to the "legitimate interest" exception, are still confusing for Canadian businesses and Canadians, and thus imperil Canada's continued "adequacy" status. Therefore, the CPPA should be revised to:*

5.1 **Strengthen valid consent in section 15 of the CPPA by restoring the "understanding" requirement in section 6.1 of PIPEDA.**

In 2015, the "understanding" requirement was added to PIPEDA (in section 6.1) as the key to the validity of consent and to ensure that consent is informed and meaningful. Unfortunately, this requirement is inexplicably absent from the CPPA. In its place is a downgraded requirement that the information provided to individuals to obtain their consent must be "in plain language that an individual to whom the organization's activities are directed would reasonably be expected to understand". Without maintaining the requirement that Canadians must be likely to understand what they have been asked to consent to, the CPPA fails to achieve its goal of giving Canadians more control over their PI. It gives them less. This failure can be remedied by restoring the following language from section 6.1 of PIPEDA to section 15 of the CPPA (e.g., see the proposed addition to section 15(3) at page 16 below):

The consent of an individual is only valid if it is reasonable to expect that an individual to whom the organization's activities are directed would understand the nature, purpose, and consequences of the collection, use or disclosure of the personal information to which they are consenting.

Underscoring the importance of this recommendation (that valid consent be strengthened by restoring PIPEDA's "understanding" requirement) are the troubling comments of Justice Manson in the Facebook Application Decision which is currently under appeal.<sup>9</sup> Specifically, Justice Manson seeks to rely on subjective evidence about users' expectations of privacy "to better assess the reasonableness

---

<sup>9</sup> See *Privacy Commissioner appeals Federal Court decision related to Facebook investigation*, Office of the Privacy Commissioner, online: [https://www.priv.gc.ca/en/opc-news/news-and-announcements/2023/an\\_230512-2/](https://www.priv.gc.ca/en/opc-news/news-and-announcements/2023/an_230512-2/)

of meaningful consent" which he suggests may be "especially context dependent and ever-evolving".

Justice Manson's comments are problematic from the standpoint of future-proofing the protection of Canadians' privacy. Such an interpretation would be at odds with the normative approach long established by the courts.

As noted by Professor Scassa in her recent blog post, the Supreme Court of Canada's 2004 [R v. Tessling](#) decision, positing that subjective expectations of privacy should not be used to undermine protections, established the normative approach applicable to Canada's privacy laws. Professor Scassa warns that it is increasingly naive to "reasonably expect" any sort of privacy in a data-hungry surveillance society with weak privacy laws.

Justice Manson's comments underscore the importance of not further weakening the meaningful consent provisions in PIPEDA. Instead, Bill C-27 should make it crystal clear that valid consent requires that it is "reasonable to expect", not subjectively but objectively, that individuals understand the nature, purpose and consequences of the collection, use, and disclosure of the personal information to which they are consenting.

**5.2 Adopt a "legitimate interests" rule that clearly ranks the individual's interests and fundamental rights above the commercial interests of the organization in any assessment of the impact of relying on the rule.**

The CPPA's proposed "legitimate interests" exception to consent should be reframed as a lawful alternative to consent, as opposed to an exception, providing that in the PIA required to be conducted by the organization an individual's interests and fundamental rights outweigh the commercial interests of the organization in collecting or using the relevant PI. This assessment rule would replace the proposed rule under Bill C-27 which provides for a balancing of commercial interests against any potential adverse effect on the individual. Transparency requirements should be included for lawful collection and use of PI without consent.

This "legitimate interests" rule would track the analogous GDPR "legitimate interests" rule that is subject always to the exception that an organization's purposes for collecting, using or disclosing an individual's PI are overridden by the "interests or fundamental rights and freedoms" of the individual.

**5.3 Eliminate implied consent as an alternative to the express consent basis for permitted collection, use, or disclosure of PI.**

When a "legitimate interest" justification is included, there is no need for "implied consent" as currently stated in s.15(5) (types of consent). There should only be one type of consent – express. If an organization cannot get express consent, then it

can rely on legitimate interests. Organizations should not have it both ways. The "implied consent" exception to express consent provided in the proposed CPPA should be eliminated. As currently stipulated, the implied consent basis conflicts with the legitimate interests exception to consent by providing for an alternative basis of permitted processing of PI "taking into account the reasonable expectations of the individual" but without the guardrails to ensure adequate privacy protections such as the PIA requirements of that rule. As provided for in Bill C-27, an organization may argue that it has implied consent for processing therefore without needing the full disclosures required for express consent nor without meeting the requirements of the legitimate interests rule, even if such processing more appropriately should be addressed by that rule.

5.4 **Require separate, opt-in consent on digital media<sup>10</sup> for collection, use or disclosure of personal information for purposes beyond what is necessary to provide a product or service.**

To address the collection of personal information on digital media beyond what is necessary to provide a product or service, organizations should be required to obtain express, opt-in consent separate from any consent given in relation to the product or service in question. Furthermore, the individual should be able to withdraw their consent at any time without impacting their receiving the product or service. Such a provision would ensure that consent to collecting personal information for advertising targeting purposes cannot be buried in the product/service's terms and conditions of use or privacy policy but must be brought to the individual's attention and obtained by separate, affirmative action by the individual.

The proposed provision is intended to capture the evolving standard for online data collection articulated in the *Meta Ireland* decisions of the European Data Protection Board on December 5, 2022 and the Irish Data Protection Commission on December 31, 2022 as well as the OPC's January 26, 2023 Home Depot Canada Report of Findings. In these cases, the reasonable expectations of the user was a key factor, as well as the "secondary use" factor.<sup>11</sup>

5.5 **Specify that the appropriate standard for determining the general impression to the average individual when ascertaining whether their consent has been obtained "deceptively" (and so is invalid) is the credulous and inexperienced person as opposed to the reasonable person.**

It is important for both Canadians and organizations that the CPPA be clear that all individuals, including those who are less sophisticated or experienced and thus more vulnerable, be protected from deceptive privacy practices. Individuals should not be misled into consenting to the collection, use, or disclosure of their PI by

<sup>10</sup> The CPPA should define "digital media" broadly to include internet, mobile, metaverse, virtual reality and other digital communications media.

<sup>11</sup> See also Quebec's Law 25, s. 8.1, which in effect requires opt-in consent for online data collection for purposes of tracking and profiling.

organizations that are not being honest. "Deceptive design patterns" (also known as "dark patterns") are misleading interface techniques for "opt-in" and "opt-out" privacy consent mechanisms that are increasingly being deployed by unscrupulous organizations to trick individuals into giving consents regarding their PI when these individuals do not intend to consent. When ascertaining whether a consent-request or other privacy practice is deceptive, the CPPA should adopt the credulous and inexperienced person test (as opposed to the reasonable person test) set in 2012 by the Supreme Court of Canada (SCC) in *Richard v. Time*, a case that concerned the test for deceptive marketing under Quebec's *Consumer Protection Act*. Specifically, as held by the SCC, the credulous and inexperienced person is someone who is trusting and hurried and neither careful nor diligent. Given the important and complex intersection of privacy law and competition law, the appropriate standard for the average individual with respect to "deceptive practices" should be the same under both laws. In this regard, notably the Competition Bureau in its March 15, 2023 submission to ISED for modernizing the *Competition Act* makes this recommendation regarding the appropriate standard for deceptive marketing practices (see recommendation 4.1 in the Bureau's submission).

- 5.6 **To address the concerns with the consent provisions raised in recommendations 5.1 through 5.5 above, sections 15, 16 and 18 of the CPPA should be revised.**

CDR suggests the following revision (a comparison follows the clean version below).

## **Consent**

### **Consent required**

15 (1) Unless this Act provides otherwise, an organization must obtain an individual's valid consent for the collection, use or disclosure of the individual's personal information.

### **Timing of consent**

(2) The individual's consent must be obtained at or before the time of the collection of the personal information or, if the information is to be used or disclosed for a purpose other than a purpose determined and recorded under subsection 12(3), before any use or disclosure of the information for that other purpose.

**Information for consent to be valid**

(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) the purposes for the collection, use or disclosure of the personal information determined by the organization and recorded under subsection 12(3) or (4);

(b) the manner in which the personal information is to be collected, used or disclosed;

(c) any reasonably foreseeable consequences of the collection, use or disclosure of the personal information;

(d) the specific type of personal information that is to be collected, used or disclosed; and

(e) the names of any third parties or types of third parties to which the organization may disclose the personal information, and

if it is reasonable to expect that the individual would understand the nature, purpose and consequences of the collection, use or disclosure of the personal information to which they are consenting.

**Plain language**

(4) The organization must provide the information referred to in subsection (3) in plain language that an individual to whom the organization's activities are directed would reasonably be expected to understand.

**Consent — provision of product or service**

(5) The organization must not, as a condition of the provision of a product or service, require an individual to consent to the collection, use or disclosure of their personal information beyond what is necessary to provide the product or service. An individual may withdraw at any time a consent given for such purposes without affecting provision of the product or service.

**Consent on digital media**

(6) Consent to the collection of an individual's personal information obtained on digital media beyond what is necessary to provide a product or service must be specific, informed and unambiguous, given by a statement or clear affirmative



action separately from any consent required for the provision of the product or service.

### **Consent obtained by deception**

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. The appropriate standard for determining whether information is false or misleading or whether practices are deceptive or misleading is the general impression of the information or practice to the credulous and inexperienced person being one who is trusting and hurried and neither careful nor diligent. Any consent obtained under those circumstances is invalid.

## **Alternative Basis for Collection and Use**

### **Legitimate interest**

18.1 An organization may collect or use an individual's personal information if the collection or use is made for the purpose of an activity in which the organization has a legitimate interest except where such interest is overridden by the interests or fundamental rights and freedoms of the individual which require protection of personal information and

- (a) a reasonable person would expect the collection or use for such an activity; and
- (b) the personal information is not collected or used for the purpose of influencing the individual's behaviour or decisions.

### **Conditions precedent**

18.2 Prior to collecting or using personal information under section 18.1, the organization must:

- (a) identify any potential adverse effect on the individual that is likely to result from the collection or use;
- (b) identify and take reasonable measures to reduce the likelihood that the effects will occur or to mitigate or eliminate them; and
- (c) comply with any prescribed requirements.

## Record of assessment

18.3 The organization must record its assessment of how it meets the conditions set out in section 18.2 and must, on request, provide a copy of the assessment to the Commissioner.

**NOTE:** For convenient reference, set forth below is a comparison showing the changes (additions in blue-underlined, deletions in ~~red-strike-through~~) CDR proposes to the current versions of sections 15, 16 and 18 (re: legitimate interest) of the CPPA.

## Consent

### Consent required

15(1) Unless this Act provides otherwise, an organization must obtain an individual's valid consent for the collection, use or disclosure of the individual's personal information.

### Timing of consent

(2) The individual's consent must be obtained at or before the time of the collection of the personal information or, if the information is to be used or disclosed for a purpose other than a purpose determined and recorded under subsection 12(3), before any use or disclosure of the information for that other purpose.

### Information for consent to be valid

(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) the purposes for the collection, use or disclosure of the personal information determined by the organization and recorded under subsection 12(3) or (4);
- (b) the manner in which the personal information is to be collected, used or disclosed;
- (c) any reasonably foreseeable consequences of the collection, use or disclosure of the personal information;
- (d) the specific type of personal information that is to be collected, used or disclosed; and
- (e) the names of any third parties or types of third parties to which the organization may disclose the personal information-, and

if it is reasonable to expect that the individual would understand the nature, purpose and consequences of the collection, use or disclosure of the personal information to which they are consenting.

### Plain language

(4) The organization must provide the information referred to in subsection (3) in plain language that an individual to whom the organization's activities are directed would reasonably be expected to understand.

**Form of consent**

~~(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 that is to be collected, used or disclosed.~~

**Business activities**

~~(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).~~

**Consent — provision of product or service**

~~(75)~~ The organization must not, as a condition of the provision of a product or service, require an individual to consent to the collection, use or disclosure of their personal information beyond what is necessary to provide the product or service. An individual may withdraw at any time a consent given for such purposes without affecting provision of the product or service.

**Consent on digital media**

(6) The consent in subsection 5 to the collection of an individual's personal information obtained on digital media for purposes beyond what is necessary to provide a product or service must be specific, informed and unambiguous, given by a statement or clear affirmative action separately from any consent required for the provision of the product or service.

**Consent obtained by deception**

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. The appropriate standard for determining whether information is false or misleading or whether practices are deceptive or misleading is the general impression of the information or practice to the credulous and inexperienced person being one who is trusting and hurried and neither careful nor diligent. Any consent obtained under those circumstances is invalid.

**Alternative Basis for Collection and Use****~~Exceptions to Requirement for Consent~~****~~Business Operations~~****~~Business activities~~**

~~18 (1) An 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 a business activity described in subsection (2) and~~

~~(a) a reasonable person would expect the collection or use for such an activity; and~~

~~(b) the personal information is not collected or used for the purpose of influencing the individual's behaviour or decisions.~~

**~~List of activities~~**

~~(2)~~ Subject to the regulations, the following activities are business activities for the purpose of subsection (1):

- ~~(a)~~ an activity that is necessary to provide a product or service that the individual has requested from the organization;
- ~~(b)~~ an activity that is necessary for the organization's information, system or network security;
- ~~(c)~~ an activity that is necessary for the safety of a product or service that the organization provides; and
- ~~(d)~~ any other prescribed activity.

#### Legitimate interest

~~(3)~~18.1 An 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~~ except where such interest is overridden by the interests or fundamental rights and freedoms of the individual which require protection of personal information<sup>212</sup> and

- (a) a reasonable person would expect the collection or use for such an activity; and
- (b) the personal information is not collected or used for the purpose of influencing the individual's behaviour or decisions.

#### Conditions precedent

~~(4)~~18.2 Prior to collecting or using personal information under ~~subsection (3)~~section 18.1, the organization must:

- (a) identify any potential adverse effect on the individual that is likely to result from the collection or use;
  - (b) identify and take reasonable measures to reduce the likelihood that the effects will occur or to mitigate or eliminate them; and
  - (c) comply with any prescribed requirements.

#### Record of assessment

~~(5)~~18.3 The organization must record its assessment of how it meets the conditions set out in ~~subsection (4)~~section 18.2 and must, on request, provide a copy of the assessment to the Commissioner.

### Exceptions to Requirement for Consent

#### Business Operations

##### Business activities

18 (1) An 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 a business activity described in subsection (2) and

---

<sup>12</sup> This revision tracks the language in the GDPR.

- (a) a reasonable person would expect the collection or use for such an activity; and
- (b) the personal information is not collected or used for the purpose of influencing the individual's behaviour or decisions.

**List of activities**

- (2) Subject to the regulations, the following activities are business activities for the purpose of subsection (1):
- (a) an activity that is necessary to provide a product or service that the individual has requested from the organization;
  - (b) an activity that is necessary for the organization's information, system or network security;
  - (c) an activity that is necessary for the safety of a product or service that the organization provides; and
  - (d) any other prescribed activity.

**~~Legitimate interest~~**

~~(3) An 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~~

- ~~(a) a reasonable person would expect the collection or use for such an activity; and~~
- ~~(b) the personal information is not collected or used for the purpose of influencing the individual's behaviour or decisions.~~

**~~Conditions precedent~~**

- ~~(4) Prior to collecting or using personal information under subsection (3), the organization must~~
- ~~(a) identify any potential adverse effect on the individual that is likely to result from the collection or use;~~
  - ~~(b) identify and take reasonable measures to reduce the likelihood that the effects will occur or to mitigate or eliminate them; and~~
  - ~~(c) comply with any prescribed requirements.~~

**~~Record of assessment~~**

~~(5) The organization must record its assessment of how it meets the conditions set out in subsection (4) and must, on request, provide a copy of the assessment to the Commissioner.~~

**6. Use all the tools in the "privacy and consumer protection toolbox" to promote accountability**

*Canada has a worthy reputation of pioneering privacy accountability measures and exporting them to other jurisdictions, including Europe. It is, therefore, very strange that some of those measures do not appear in the CPPA. Accordingly, several provisions of Bill C-27 should be*

*enhanced to promote organizational accountability and to ensure Canada's "adequacy" determination is maintained.*

- 6.1 **Require organizations to conduct privacy impact assessments (PIAs) in advance of product or service development - particularly where invasive technologies and business models are being applied, where minors are involved, where sensitive PI is being collected, used, or disclosed, and when the processing is likely to result in a high risk to an individual's rights and freedoms.**

PIAs are an established instrument in privacy and data protection regimes, and a critical component of demonstrable accountability for personal data governance. They are required under certain conditions under the GDPR and Quebec's Law 25. They are also required under several provincial public sector laws. They are good business practice, and many organizations already conduct them as a part of their privacy management programs. In the context of the CPPA, they would bolster the accountability provisions. They would also help ensure that, where a business is relying on one of the exceptions to the requirement for consent, the business has thoroughly assessed the privacy implications of its activities. They should be expressly required by the CPPA.

- 6.2 **Expressly require organizations to protect (i) privacy by "default" to align with Quebec's Law 25, section 9.1 and (ii) personal data by "design and default" to align with the GDPR, Article 25 (to help ensure "adequacy").**

This can be accomplished by adding to section 57(1) of the CPPA a requirement that an organization's security safeguards must, by "default", ensure that only an individual's PI that is necessary for each specific purpose of the collection, use or disclosure is indeed collected, used or disclosed by the organization. This is especially important with respect to organizations that offer technological products or services to the public, who should (as in Quebec) be required to provide the highest level of security, without intervention by the user.

Such "privacy by default" protection should include developing and implementing a governance framework of "control by design" (**CbD**) shifting the governance of PI from the designers of technology and their self-policing practices to democratically accountable powers (**DAPs**) – thus, enabling Canadians to oversee and control their PI. Under the CbD governance framework, significant personal information datasets would be controlled by DAPs responsible to Canadians (both individuals and groups). For more detail on the reasons for and nature of CbD, please see Recommendation 11.1 in Appendix B.

- 6.3 **Promote the development of data stewardship models.**

The CPPA should include a provision that promotes the development of data stewardship models whereby information, both personal and non-personal, may be

provided to a data steward or facility (or possibly a central data utility) authorized to make such data available to parties interested in using the data, in a protected manner, for designated purposes including leveraging economic opportunity, research, public sector planning, and social benefit. Such a model would be more clearly broader in scope than the CPPA's definition in section 39(2) of "socially beneficial purpose" (i.e., "a purpose related to health, the provision or improvement of public amenities or infrastructure, the protection of the environment or any other prescribed purpose") and not restricted to public sector entities. Especially as data stewardship models are still experimental, any such authorizations need to be based on a PIA, should only be granted in advance for a limited time period (renewable), and be subject to retrospective independent review to ensure that the designated purpose is achieved in practice.

#### 6.4 **Strengthen security safeguards.**

Specifically, require organizations to take into account the potential consequences, to both individuals and society, through measures such as PIAs, of a breach of security safeguards in addition to taking into account, as already set forth in section 57 of the CPPA, the sensitivity, quantity, distribution, format, and method of storage of the information.

The recent Facebook Application Decision contains observations that, as described by Professor Scassa, "should set off alarm bells with respect to Bill C-27". In particular, the decision states that PI safeguarding obligations end after the PI has been disclosed to a third party. This interpretation is partly based on the existence of the carve-out in PIPEDA for business transactions, where PI can be used and disclosed without consent in the context of a business transaction, provided that the transaction parties enter into an agreement to the effect that the receiving party (purchaser) will continue to apply safeguarding obligations to the PI disclosed. As pointed out by Professor Scassa, further safeguarding provisions may be necessary in Bill C-27 to address, for example, PI that can be disclosed without the knowledge or consent of the individual in certain circumstances, such as for socially beneficial purposes under section 39. Bill C-47 should include a requirement that organizations disclosing PI (including de-identified information) without consent for the specific permitted purposes such as socially beneficial purposes must put in contractual provisions to safeguard PI following disclosure.

#### 6.5 **Like Quebec's Law 25, the CPPA should have a separate section for cross border data flows requiring that organizations in Canada that export PI to a foreign jurisdiction for processing must first conduct a PIA to establish that the PI will receive an equivalent level of protection as in Canada.**

There is no express section in Bill C-27 dedicated to the vital issue of cross-border data flows. Despite multiple recommendations from experts, Bill C-27 continues to ignore the reality that transfers to service providers nationally is a different context than transferring to service providers internationally. It is not as if Bill C-27 does not recognize the pervasive and rapid exchange of data between countries – its preamble specifically states that Canada is a trading nation, reliant on the exchange of PI and data across borders. The deliberate omission of a dedicated section, or even any substantive relevant provisions to address this issue is a serious shortcoming of Bill C-27 that could be addressed by looking to other comparable jurisdictions, including Quebec's Law 25.

As in Quebec, any additional risks should be identified, justified, mitigated and documented in a PIA. As well, the PIA should include an assessment of the broader level of privacy and human rights protection in the foreign jurisdiction, including how Canadians' privacy rights can be enforced. If Canada's adequacy status is maintained, it will be much easier for businesses to prepare such PIAs when sending Canadian PI to the EU.

**6.6 Adopt a more comprehensive regime governing third party data processors/service providers.**

The CPPA should establish a comprehensive regime governing third party data processors/service providers, stipulating minimum contract requirements, directly imposing obligations on them, comparable to the GDPR, including accountability-compliance requirements beyond simply security, as is proposed in the CPPA. As well, this regime should distinguish between PI flows entirely within Canada and those from Canada to another country and provide for stricter privacy protections for PI flows that cross international borders.

**6.7 Clearly impose transparency and accountability obligations on data brokers.**

Data brokers (i.e., third parties who are not service providers) are a largely invisible and highly problematical aspect of the surveillance business model and the AdTech industry ecosystem. The CPPA should include specific rules applicable to data brokers in order to ensure that this data trafficking sector is regulated effectively under federal private sector privacy law. Consistent with the EU's *Data Governance Act* (that has been applicable since September 1, 2023), a fiduciary duty to individuals should be imposed on all intermediaries within data supply chains to ensure that data brokers only use PI entrusted to them for the purposes intended by the individuals to whom the PI relates. In addition, the CPPA should oblige data brokers to make their roles more visible by requiring them to pass their identity downstream in the data supply chain (and/or possibly some official registration requirement – e.g., along the lines of the registry proposed in recommendation 11.3 below and similar to the requirements in the proposed United States *DELETE*



*Act*<sup>13</sup>).<sup>14</sup> In this way, if an individual is adversely affected by the transfer or use of their PI in the data supply chain, they can determine which data brokers handled their PI. Parliament could do well to look to the EU's *Data Governance Act* and the role of data intermediaries as an alternative model to Big Tech, where data intermediation services providers that intermediate the exchange of data need to register publicly and bear a fiduciary duty to ensure that they act in the best interests of data subjects.

## 7. **Strengthen individuals' control over their PI**

*Changes are needed to Bill C-27 in order to ensure that individuals can effectively port, delete, and access their data (in keeping with Canada's objective of maintaining its "adequacy" status). Canadians should also be able to contest the decisions made about them by ADS/AI systems as well as have a private right of action in the event of privacy violations. Therefore, CDR recommends that the CPPA:*

### 7.1 **Provide for a more comprehensive right to PI "mobility" (aka "portability").**

The CPPA proposes a right granted to individuals only in the context of "data mobility frameworks" that is limited in two key respects: first, the PI that can be ported is limited to that which the organization itself has collected from the individual; and second, the individual's PI gets transferred from the organization that collected the PI to another organization designated by the individual. An individual should be able to receive their PI from the organization directly in order to (1) maximize the individual's control over their PI, (2) encourage competition and support innovation, and (3) align with the GDPR (and be interoperable with the individual's right to data mobility/portability under the law in Quebec coming into force on September 22, 2024). Moreover, an individual should also have the right to port any PI that the individual has provided to an organization such as by

---

<sup>13</sup> Under the proposed United States' federal *Data Elimination and Limiting Extensive Tracking and Exchange Act*, the [DELETE Act](#), every registered data broker that maintains any "persistent identifiers" (such as emails, phone numbers, physical addresses) will be required to pay to the Federal Trade Commission an annual subscription fee determined by the FTC, to access the Centralized Data Deletion System database. The FTC's chosen subscription fee may not exceed 1% of the expected annual cost of operating the centralized system and hashed registries, as determined by the FTC (s.2(b)(3)(B)).

<sup>14</sup> Similarly, on September 14, 2023, the California Legislature passed the [Delete Act](#) (Senate Bill 362) that requires all data brokers to register for a fee with the California Privacy Protection Agency (CPPA). Once signed by the Governor, the California Act will require the CPPA to create a public "delete mechanism" by January 1, 2026, through which a consumer (or an authorized agent) can submit a single verifiable request that every data broker delete the consumer's personal information. Starting August 1, 2026, data brokers will have to access the delete mechanism at least once every 45 days and, within 45 days of receiving a request, delete the consumer's personal information (subject to limited CCPA deletion exemptions). Beginning January 1, 2028, and every three years after, data brokers will have to undergo an audit by an independent third party to ensure compliance with the Act. Data brokers will be obliged to keep records of all compliance audits for at least six years and to submit such records to the CPPA upon request. As of January 1, 2029, data brokers will have to disclose their audit results when registering with the CPPA.

completing online forms or by the organization observing the individual's online activity.

7.2 **Limit the exceptions to the right to "disposal" of PI (aka a right to "deletion"/"erasure"/"be forgotten") and provide for a right to disposal with respect to search engines' indexing of individuals' PI in specified circumstances.**

The right to disposal should not be subject to exceptions that limit unreasonably the potential scope of the provision including use in connection with the provision of a product, reasonable bulk requests for deletion, and an organization's record retention schedule. The right to disposal should apply to online platforms in respect of their indexing of PI through online search engines in specified circumstances such as illegality or harm to an individual's privacy or reputation, subject to the public right to freedom of expression.

7.3 **Strengthen information and access.**

Specifically, in section 63 of the CPPA, restore the language and intent of PIPEDA Principle 9 (i.e., 4.9.3) regarding Individual Access as follows:

4.9.3 In providing an account of third parties to which it has disclosed personal information about an individual, an organization should attempt to be as specific as possible. When it is not possible to provide a list of the organizations to which it has actually disclosed information about an individual, the organization shall provide a list of organizations to which it may have disclosed information about the individual.

7.4 **Prohibit, subject to specific and narrow exceptions, organizations from using ADS/AI to collect, use or disclose an individual's PI as the basis for decisions about them to align with GDPR, Article 22 (to help ensure "adequacy").**

Specifically, add a section to the CPPA providing individuals with a right not to be subject to a decision based solely on ADS/AI which produces legal effects on them or similarly significantly affects them, subject to the following exceptions: (a) the decision is necessary for a contract between the individual and the organization, (b) the decision is otherwise authorized by law, or (c) the individual has expressly consented to the decision. In addition, the CPPA should take into account any privacy protection enhancements for individuals that ban an organization's use of ADS/AI in connection with PI, akin to those that were proposed in the European Commission's April 2021 *Proposal for a Regulation Laying Down Harmonized Rules on AI* (the **EU AI Act**). On June 14, 2023, Ministers of the European Parliament adopted the EU AI Act as the basis for AI legislation in EU member

states.<sup>15</sup> The EU AI Data Act bans ADS/AI systems that pose an unacceptable level of risk, or are intrusive or discriminatory. The ban includes systems that:

- deploy subliminal or purposefully manipulative techniques;
- exploit people's vulnerabilities, are used for social scoring (such as classifying people based on their social behavior, socio-economic status, or personal characteristics);
- use "real time" remote biometric identification systems in publicly accessible spaces, such as facial recognition;
- use "post" remote biometric identification systems, with the only exception being law enforcement for the prosecution of serious crimes and only after judicial authorization;
- deploy biometric categorisation systems using sensitive characteristics (e.g., gender, race, ethnicity, citizenship status, religion, and political orientation); predictive policing systems (based on profiling, location or past criminal behaviour);
- use emotion recognition systems in law enforcement, border management, workplace, and educational institutions; and
- involve indiscriminate scraping of biometric data from social media or CCTV footage to create facial recognition databases (violating human rights including the right to privacy).<sup>16</sup>

The EU AI Act also identifies areas that pose a high risk to people's health, safety, fundamental rights, or the environment. These include AI systems used to influence voters in political campaigns and in recommendations systems used by social media platforms.

#### 7.5 **Give individuals the rights to contest and object to ADS/AI affecting them, not just a right to "algorithmic transparency".**

This can be accomplished by including specific provisions to ensure "responsible" innovation and "responsible" ADS/AI such as: (1) a more clearly articulated right of individuals to a meaningful explanation than is set forth in section 63(3) of the CPPA (such as "an explanation that allows individuals to understand the nature and elements of the decision to which they are being subject or the rules that define the processing and the decision's principal characteristics") and including a requirement that the organization provide disclosures of the legitimacy, accuracy, reliability, reasonably foreseeable consequences, potential risks, mitigations, and safeguards of the ADS/AI process; (2) as necessary, complements the right to an

---

<sup>15</sup> See "EU AI Act: first regulation on artificial intelligence", European Parliament, June 14, 2023, online: <https://www.europarl.europa.eu/news/en/headlines/society/20230601STO93804/eu-ai-act-first-regulation-on-artificial-intelligence> .

<sup>16</sup> European Parliament, press release, "AI Act: a step closer to the first rules on Artificial Intelligence", <https://www.europarl.europa.eu/news/en/press-room/20230505IPR84904/ai-act-a-step-closer-to-the-first-rules-on-artificial-intelligence> .

explanation, (a) the right of individuals to express their point of view to a human intervenor and contest the decision (whether the individuals have consented or the organization has relied on an exception to consent) and (b) the right of individuals to object to/withdraw consent regarding the decision; and (3) the obligation on organizations using AI to provide demonstrable accountability (i.e., requiring them to log and trace their collection and use of PI in connection with the complex processing by their AI systems), and giving the Privacy Commissioner powers to audit and inspect these records and practices. These enhancements to the CPPA's incomplete ADS/AI provisions are described more fully in the Privacy Commissioner's November 12, 2020 report *A Regulatory Framework for AI: Recommendations for PIPEDA Reform*.

#### 7.6 **Strengthen the private right of action (PRA).**

This can be accomplished by removing the pre-conditions to the exercise of the private right of action provided for in section 107 of the CPPA – namely, that either (1) the Privacy Commissioner has made a finding that there has been a contravention of the CPPA by the organization and the finding has not been appealed by the organization, or the Personal Information and Data Protection Tribunal (**Tribunal**) has dismissed the organization's appeal of that finding, or (2) the Tribunal has made a finding that the organization has contravened the CPPA. The time and cost required to fulfill these pre-conditions will deny access to justice for most individuals under the PRA. Courts have greater expertise than the Commissioner or the Tribunal in hearing evidence and making findings of fact and rulings on liability. It is the courts, not the Commissioner, that will make binding decisions that develop the law of civil liability for breach of the CPPA. Thus, neither the Privacy Commissioner nor the Tribunal should act as a gatekeeper for the PRA. Frivolous or vexatious claims brought by individuals or by a proposed class can be dismissed under the rules of procedure available in the Courts.

The most straightforward approach would be to adopt a simple provision along the lines of section 36 of the *Competition Act* (which gives a remedy to any person who has suffered loss or damage as a result of a contravention of the criminal provisions of the Act with no pre-conditions). The remedy under the CPPA's proposed PRA is limited to "damages for loss or injury that the individual has suffered" as a result of a contravention. The remedy should be expanded to include "moral damages" since most contraventions will not result in a provable pecuniary loss. Consideration should also be given to provide for minimum statutory damages for contraventions of the CPPA. Individuals should also be granted the right to seek an injunction to enjoin continuing contraventions of the CPPA. As well, the CPPA should clarify that it is not a "complete code" and shall not be construed as depriving any person of any civil right of action (i.e., individuals may still sue organizations for privacy violations at common law in contract, tort or other legal ground). To ensure the Commissioner's involvement, it may help to give the Commissioner a right of notice of any private action and a right to intervene in it.

- 7.7 **Adjust the CPPA's proposed regime for non-identifiable information (i) to make clear that organizations must apply appropriate processes to de-identify information and protect any such information and (ii) to provide that anonymized information complies with standards set out in regulations, to align with Quebec's Law 25.**

The definition of "de-identify" should be amended to stipulate that appropriate processes, as prescribed by regulation, be required to ensure that no person can be directly identified from the information. The definition should reflect that information is de-identified if it is stripped of direct identifiers in accordance with standards set by regulation or by adding a specific reference in the definition to section 74. Section 74 should be amended to require that technical and administrative protections must be applied to all de-identified information. The regime would stipulate requirements regarding the processes for anonymization as well as the guardrails including transparency and accountability obligations to maintain the non-personal status of the resulting information in downstream uses. Furthermore, the regime must reflect the reality that truly "anonymized" data is practically impossible for any dataset; the definition of anonymized information should be amended to reflect this reality, to align with Quebec's Law 25. The regulatory regime must include provisions for PIAs and independent review to ensure compliance.

These recommended amendments to the Bill C-27 provisions regarding non-identifiable information are consistent with, but go beyond, the December 7, 2022 **Submission on Bill C-27** of the Canadian Anonymization Network (**CANON**) in addressing protective requirements for de-identified and anonymized information.

## 8. **Give the Privacy Commissioner more teeth and bite**

*The Tribunal model proposed in Bill C-27 is ill-conceived, unprecedented, unjustified, costly and confusing. Bill C-27 needs to modernize its proposals and bolster the pre-existing compliance and enforcement structure of the Office of the Privacy Commissioner of Canada.*

### 8.1 **Scrap the proposed Personal Information and Data Protection Tribunal.**

The proposed introduction of the Tribunal is ill-conceived and without apparent justification. It will only introduce unprecedented and unnecessary complexity, delay and uncertainty for both individuals and organizations in the resolution of a complaint. This complexity, delay and uncertainty could undermine the clout of the Privacy Commissioner in the eyes of individuals to effectively and definitively protect their privacy rights. It may also undermine the trust organizations might otherwise have in the Privacy Commissioner to establish a level playing field for all organizations in their compliance with the CPPA. That said, if the Tribunal is scrapped, the CPPA must, in light of the significant penalties and other orders that are being contemplated, include strong provisions for due process and judicial oversight.

No justification (privacy law innovation or otherwise) has been given for the Tribunal. Its assigned role and composition raise serious concerns (including unnecessary complexity, delay and uncertainty for both individuals and organizations in the resolution of a complaint). Further, there is no privacy law regime in the world (including the modern and progressive regime in the EU, as well as the regimes in California, Utah, Colorado, Virginia and Connecticut, and the proposed *American Data Privacy and Protection Act*) that has established a tribunal like the Tribunal being proposed under the PIDPTA. Nor is such a tribunal proposed in the Australian Government's February 16, 2023 Privacy Act Review Report 2022. Moreover, the introduction of the Tribunal would cause unnecessary delay and complexity in the resolution of privacy complaints.<sup>17</sup>

## 8.2 **Provide for more flexible enforcement.**

Although section 94 of the CPPA stipulates some general factors that must be taken into account in setting administrative monetary penalties (**AMPs**) and fines, these should be expanded to include all specific and relevant aggravating and mitigating factors stipulated in other federal statutes aimed to protect Canadians (such as in *Canada's Anti-Spam Legislation (CASL)* and the *Competition Act*). These factors could include the frequency and duration of the conduct and the vulnerability of the persons affected. As well, the factors for setting AMPs and fines should specifically include the sensitivity of the PI for which the organization contravening the CPPA is responsible. This flexibility will allow for more tailored and effective enforcement against all organizations whether big or small. It will also be more responsive to the diversity of small and medium-sized enterprises in the Canadian economy.

## 8.3 **Equip the Privacy Commissioner with the power to seek the imposition of administrative monetary penalties (AMPs) in a manner similar to the powers of the Commissioner of Competition under the *Competition Act*.**

The Privacy Commissioner must have the ability to apply to the courts for specific amounts of AMPs against bad actors, rather than being limited only to making recommendations to the Tribunal (as is currently the case under the CPPA). The ability to apply for AMPs is a natural complement to the injunction-like compliance order-making powers of the Privacy Commissioner and will allow for certain matters to be resolved in a more expeditious and timely manner. Similar to the Commissioner of Competition's power to do so, the Privacy Commissioner also should clearly and expressly be able to negotiate a financial payment by an

---

<sup>17</sup> For example, the UK Information Commissioner's Office (**ICO**) commenced an investigation in 2018, resulting in an Enforcement Notice to Experian in 2020. Experian appealed the matter to the UK First Tier Tribunal – the matter was heard by that tribunal in 2022, and the tribunal's decision was given in February 2023 – nearly 5 years after the commencement of the investigation. And the matter could continue to be ongoing since the ICO must decide whether it will appeal the decision.

organization as part of a compliance agreement that, in turn, is approved by the courts on consent of both parties.

- 8.4 **Empower the Privacy Commissioner to issue "enforcement notices" and expand the sections for which the Privacy Commissioner can recommend penalties to include violations of the following: 12(1) (Appropriate purposes); 55 (3) (Disposal at individual's request: Reasons for refusal); 73 (Complaints and requests for information); 75 (Prohibition on re-identification); and 97 (Audits).**

The CPPA should empower the Privacy Commissioner to issue an "enforcement notice" to an organization where the Privacy Commissioner is satisfied that the organization has failed to comply with certain core obligations under the CPPA. This notice will give the organization a specified period of time within which it must comply (absent appeal of the notice), failing which the Privacy Commissioner may issue a "penalty notice" imposing such requirements as the Privacy Commissioner may deem appropriate for the purpose of remedying the non-compliance and failure, including an AMP. This power could be modelled on the power to issue enforcement and penalty notices granted to the United Kingdom (UK)'s Information Commissioner under sections 149, 150 and 155 of the *UK Data Protection Act, 2018*.

- 8.5 **Strengthen the inter-agency collaboration and information-sharing provisions between the Privacy Commissioner, the Commissioner of Competition, and the CRTC.**

The CPPA, the *Competition Act* and the *Canadian Radio-television and Telecommunications Commission Act* should permit information sharing and co-operation among the Privacy Commissioner, the Commissioner of Competition and the CRTC relevant to their respective duties, powers and functions under that legislation and for the effective administration of their relevant legislation in the manner similar to that provided under CASL. The legislation should permit consultation among all three regulators, including requiring collaboration when receiving foreign information requests. As currently written, the CPPA provides only for permissive information sharing and joint research between the Privacy Commissioner on one hand and the Commissioner of Competition, or the CRTC, on the other hand. The collaboration provisions in the legislation should provide for three-way information sharing and collaboration.

- 8.6 **Strengthen the whistleblowing regime.**

The Privacy Commissioner's protection of the confidentiality of the whistleblower and the prohibition against an employer taking retribution against a whistleblowing employee in sections 126 and 127, respectively, of the CPPA are necessary but insufficient. To encourage employees to report bad behaviour, a whistleblower should be entitled to a discretionary award based on a percentage of total monetary

sanctions recovered from, or voluntary payments made by, the offender. As well, consistent with the EU *Whistleblower Directive*, the CPPA's whistleblower provisions should be enhanced to include (1) a limitation of liability of the whistleblower (i.e., that they shall not incur liability of any kind in respect of whistleblowing provided they had reasonable grounds to believe that the whistleblowing was necessary for revealing a breach) and (2) a "reverse onus" of proof on the organization (i.e., when there are legal proceedings in relation to a detriment suffered by a whistleblower, it shall be presumed that the detriment was made in relation to the whistleblowing). This reverse onus places a significant responsibility on organizations to demonstrate that any action taken after the whistleblowing was not done for retaliation purposes.

#### 8.7 **Implement a self-reporting program for organizations.**

The CPPA should implement a self-reporting program that offers immunity or lenient treatment for organizations that are parties to agreements that contravene the CPPA. Providing incentives to parties to come forward and seek immunity or leniency in exchange for cooperation with any investigation will enhance the detection, investigation, and prosecution of such agreements that might otherwise remain uncovered. In addition, self-reporting programs may extend immunity or lenient treatment to the directors and officers of an organization that has been party to an agreement that violates the CPPA, which may encourage individuals to disclose information and cooperate without fear of personal liability being imposed on them or others.

#### 9. **The *Artificial Intelligence and Data Act (AIDA)* is foundationally flawed, needs proper consultation, and should be sent back to the drawing board (but don't leave it to ISED alone).**

*AIDA is simply not ready and needs proper consultation to tackle the demands of today and tomorrow. ISED's belated publication on March 13, 2023, of its "companion document" in an effort to provide some clarity to the government's AIDA introduced on June 16, 2022, does not fix these fundamental flaws. For the reasons set forth in Appendix F, ISED's companion document leaves no doubt that "No AIDA is better than this AIDA".*

*Likewise, ISED's consultation in August and September 2023 on the draft Canadian Guardrails for Generative AI – Code of Practice was problematical for the reasons set forth in Professor Clement's open letter to the ISED Minister available [here](#).*

##### 9.1 **AIDA is improper and incomplete.**

The addition of AIDA to the proposed Bill C-27 is surprising due to its lack of consultation and exclusion from failed predecessor former Bill C-11. Much of the substance of the proposed law is left to currently undeveloped regulations, forcing Parliament to enact a law without understanding its true scope and application. This incompleteness extends to crucial definitions within AIDA such as "high impact



systems", a concept which narrows the obligations of actors from the proposed and comparable EU AI Act. The proposed law's restricted application to the trade and commerce context and exclusion of federal government institutions and other actors assures that important gaps will exist in Canada's AI regulation framework.

The promise of consultation at the regulation-development stage is not a remedy for lack of consultation with respect to the framework established in the legislation. There has been no consultation, for example, on the role that the Minister is to play under the legislation, on the role of the Data Commissioner, on the definition of "harm", and on other key features of the proposed law. The lack of consultation means that the potential impact and implications of this draft – which is difficult to understand with so many of its features left to regulation – are poorly understood. This is not acceptable.

## 9.2 **AIDA inappropriately focuses excessively on risks of harms to individuals to the exclusion of collective harms.**

The proposed law defines high risk AI systems in terms of their impacts on individuals, not groups and communities. It considers impacts more narrowly than the proposed EU AI Act and the federal government's own *Directive on Automated Decision Making*. Despite introducing the notion of "biased output", AIDA's focus on individual and quantifiable harms may unwittingly help perpetuate denials of systemic discrimination. AIDA's goals are necessary and important, but it significantly underperforms due to its individualistic focus, which runs counter to global understandings of collective harm.

The types of harms that AIDA considers are: physical or psychological harm to an individual, damage to an individual's property, or economic loss to an individual. However, AIDA leaves ambiguous what could be determined a quantifiable harm. For example, one could envision an AI system that profiles individuals, pursuing their personal susceptibilities in order to target them advertisements or generally prey on perceived human weaknesses. Firstly, because AIDA lacks a definition of a high impact system, it is unknown whether this kind of system would fall within that definition. Secondly, it is not clear that manipulative and exploitative algorithms would be found to cause "harm" within AIDA's definition. Under AIDA, the harm resulting from AI systems stands difficult to quantify.

Effectively addressing "harm" under AIDA should also include imposing obligations on persons responsible for high-impact systems to establish measures to identify, assess and mitigate the risks of harm or biased output that could result from the use of the system. Furthermore, persons responsible for high-impact systems should be required to notify the responsible Minister if the use of the system results or is likely to result in material harm (for example, where material harm has occurred or is about to occur).

### 9.3 **AIDA possesses contradictory language and fragile enforcement powers.**

The treatment of anonymized data between the CPPA and AIDA creates a significant governance gap in scope, substance and process. Further, definitional limits ported into AIDA from the CPPA are not relevant, such as the definition of "personal information". Enforcement mechanisms, including the lack of a private right of action or complaint mechanism, are also incomplete. The lack of a real, independent regulator under AIDA goes against the advice of the OECD on AI governance. The lack of detail in AIDA's oversight and enforcement scheme is alarming and the government's goal of agility should not be confused with slapdash.

### 9.4 **AIDA inappropriately focuses on an overly narrow range of algorithmic techniques.**

AIDA only regulates the use of an "artificial intelligence system", which it defines as "a genetic algorithm, a neural network, machine learning or another technique." This is far narrower than the much more inclusive definition found in the proposed EU AI Act, which covers a wide range of algorithmic techniques including those that have been in widespread use for decades. AIDA therefore misses many of the potential harms it is presumably intended to cover, such as those caused by algorithmic amplification of divisive, hateful, sensationalist or politically manipulative messaging, which do not necessarily depend on the small set of sophisticated, novel techniques listed in its definition of AI.

### 9.5 **Go back to the drawing board on AIDA, but don't leave it to ISED alone**

#### **a) Parliamentarians, lead the way**

Given the pervasive confusion over the nature of 'artificial intelligence,' intensified by highly publicized hyperbolic claims of its capabilities, potential benefits and prospective harms, the initial task is one of education, both of legislators and the public more generally. Industry experts, researchers, lawyers, and civil society organizations, especially those representing stakeholders and communities most likely to be at risk, have much to offer in clarifying the issues at hand.

AIDA needs further and proper consultation to tackle the demands of today and tomorrow. To help ensure such consultation, an all-party parliamentary working group could be struck to address AIDA's general principles, framework, appropriate governance, oversight mechanisms, definition of high impact AI systems, and possible no-go zones. This should involve commissioning background research reports, publishing a White Paper and convening a genuine public consultation. Akin to the EU AI Data Act, some of the more technical aspects of AI regulation could be left to experts and addressed in the regulations under AIDA or in industry standards.

## b) Step up Federal Government

Implementing AI systems at scale can have wide societal consequences well beyond the scope of ISED's mandate. This implies other government ministries and agencies also need to play a formative role in crafting AIDA. Such government-wide collaboration can build on current work led by Justice Canada and Global Affairs Canada, supported by Treasury Board Secretariat and ISED in Canada's negotiations with the Council of Europe (COE) to develop a treaty on AI that prominently values human rights, democracy and the rule of law. The [Consolidated Working Draft of the Framework Convention](#) provides useful material for Canada's own AI regime. Canada's AI regulatory regime should conform to the convention once ratified. However, the draft convention's general provisions, obligations and principles are better aligned with the goals of avoiding harm, building trust and advancing the public interest than anything ISED has made public so far. Other obvious ministries with contributions to make include Employment and Social Development Canada (labour), Public Safety (cyber security) and Canadian Heritage (content creators and artists). The Office of the Privacy Commissioner also has an important but so far neglected role to play.

## c) Convene a National Citizens' Assembly on AI Governance

The public consultation could take the form of a well-publicized National Citizens' Assembly on AI Governance. It would report to and be coordinated with the parliamentary working group for sharing of testimony and other materials. The OECD recommends Citizens' Assemblies as offering a path to meaningful citizen engagement and evidence-based decision-making for tackling complex and challenging issues. Such Assemblies have been used successfully in many jurisdictions including Canada.<sup>18</sup> The recently completed Canadian Citizens' Assemblies on Democratic Expression, which examined the impact of digital technologies on Canadian society,<sup>19</sup> could provide a valuable model for an Assembly on AI Governance. Another example is the British Columbia User panel in relation to the British Columbia Services Card. Experience with this panel suggests that citizens' expertise meaningfully contributes to enhancing the understanding of privacy and tech issues.<sup>20</sup>

Although AI regulation can be highly technical, some of the more technical aspects can be left to regulations and standards where expert knowledge has a more prominent role to play. But the law itself should contain principles, appropriate governance and oversight mechanisms, key definitions, such as high-impact or high-risk AI, and possibly even some no-go areas – all things that citizen assemblies

<sup>18</sup> See A National Citizens' Assembly on Electoral Reform. Citizen Assemblies on Electoral Reform have been conducted in BC (2004) and Ontario (2006) and recently approved as federal Liberal Party policy.

<sup>19</sup> See [Democratic Expression Démocratique](#)

<sup>20</sup> See, "Recommendations from BC Services Card User Panel", online: <https://engage.gov.bc.ca/app/uploads/sites/121/2017/02/Appendix-II-Recommendations-from-BC-Services-Card-User-Panel.pdf>

and parliamentary committees can and should address.<sup>21</sup> Indeed, given the rapid pace of technological change, a principled approach to drafting legislation and regulations, with appropriate transparency and accountability measures, rather than one tied to specific technologies, is necessary for any legally-enforced rules to be broadly understood and accepted, and durably viable over time.

#### **d) Scope AI and its potential risks broadly**

To encourage an adequate airing of AI issues, the scope of deliberations should adopt an expansive view of what constitutes AI and its socioeconomic implications, particularly in relation to its potential harms. Restricting the definition of AI to specific algorithmic techniques, as AIDA currently does, shifts attention away from the core issues. The latest version EU's AI Act, passed recently by the European Parliament's leading parliamentary committees, offers a much more suitable starting point:

“‘Artificial intelligence system’ (AI system) means a machine-based system designed to operate with varying levels of autonomy and that can, for explicit or implicit objectives, generate outputs such as predictions, recommendations, or decisions, that influence physical or virtual environments.”<sup>22</sup>

AIDA focusses narrowly on individual and quantifiable harms. Adequately understanding and resolving the controversies currently swirling around AI requires a much broader approach to identifying risks that need to be regulated. A partial sample includes such concerns as job loss/displacement, societal discrimination, behaviour manipulation, mental health disturbance, economic deprivation, labour exploitation, cyber weaponry and autonomous lethal arms (aka “killer robots”), public mis-spending, environmental degradation, privacy abuse, intellectual property theft, public safety and security threats from accelerated cybercrime, automated blackmail, revenge porn and other scams,<sup>23</sup> election interference, power concentration and erosion of democracy. And this doesn't include the much touted but speculative 'existential' risks of an AI takeover of humanity.

Many of these risks are better treated as collective rather than individual harms. Collective harms are unevenly distributed across society and can be very significant

---

21 Note that while technical expertise is a necessary ingredient in establishing regulations and setting standards it alone is insufficient, especially in the case of powerful technologies such as AI, where advancing the public interest and protecting fundamental human rights are at stake. Those who bring complementary expertise in such areas as good governance, human rights and social impact assessment or represent communities most likely to be affected must be included, supported and given an effective say in the bodies that define regulations and standards. See Mehwish Ansari and Vidushi Marda (2023 May 5) [AI Act — leaving oversight to the techies will not protect rights](#), *euobserver*

22 Luca Bertuzzi (2023, May 11) [AI Act moves ahead in EU Parliament with key committee vote](#), *EURACTIV*.

23 Drawn from such widely circulated referenced articles and videos, such as [The AI Dilemma](#), The Stochastic Parrot.

in their cumulative effect. Typically, they cannot be attributed to singular causes nor readily quantifiable. This calls for more systemic evaluative approaches more akin to environmental impact assessment, with wide stakeholder involvement, than more individualistic methods.

#### e) Collaborate and align internationally

Given the vast scale of the most prominent AI systems and the global reach of their corporate promoters, it is widely recognized that AI regulations need to be aligned internationally. Canada already participates in two international AI policy initiatives – the OECD AI Policy Observatory ([OECD.AI](#)) and the related Global Partnership on Artificial Intelligence ([GPAI](#)). While Canadians from several sectors, including academia, business, civil society/NGO, government, and technical, are active in these organizations, it appears Canadian parliamentarians are absent.<sup>24</sup> Participation by at least a few Canadian parliamentarians in one or both of these organizations would be valuable, both for self-education and to bring a new perspective to international policy development. One recent proposal that parliamentarians might help shape and want to align Canadian AI laws with is the establishment of an international AI regulatory agency.<sup>25</sup>

Canadian parliamentarians could also contribute directly to greater international alignment of AI policy and legislation by joining efforts with legislators in other jurisdictions. One particularly important initiative that Canadian parliamentarians may want to support is the recent call by EU lawmakers for an EU/US summit to control 'very powerful' AI.<sup>26</sup> If that goes ahead, Canada should not be left out.

### C. Summary and Conclusion

Bill C-27 is not fit for purpose. Canada deserves much better for the protection of personal information. Bill C-27 continues to fall short in addressing the serious privacy challenges that have emerged over the past two decades since PIPEDA was enacted. It fails to address the reality that dominant data-driven enterprises rely on monetizing personal information through mass surveillance of individuals and groups. This model has produced a new generation of tech giants of unprecedented size and reach and exacerbated the power asymmetries these organizations already had with data subjects. Like it or not, the GDPR is widely seen as the *de facto* global standard for international data protection, and many large companies are already having to comply with its provisions to the extent that they operate in Europe or process data on European citizens. Bill C-27 does not align with contemporary global standards or the current reality of personal data flows.

---

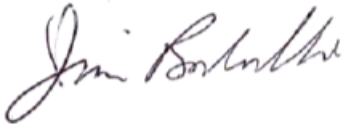
24 The OECD AI Observatory lists its 433 members [here](#), but the GPAI has yet to do the same.

25 Gary Marcus and Anka Reuel (2023 April 18) [The world needs an international agency for artificial intelligence, say two AI experts](#), *The Economist*.

26 Martin Coulter and Supantha Mukherjee (April 17, 2023) [EU lawmakers call for summit to control 'very powerful' AI](#). *Reuters*.

Parliament should not presume that Bill C-27 will meet the heightened bar of "essential equivalence" when the CPPA is assessed for adequacy. The opportunity to get Canadian federal privacy legislation right is now. It is therefore urgent for Parliament to fix these problems and thus provide Canadians with effective protection of their privacy rights and hold organizations accountable. Many of the recommendations in this Report draw on examples from leading jurisdictions where better privacy protection and responsible innovation are mutually reinforcing. Others are truly made-in-Canada innovations (including, for further study, one to develop and implement a new and robust *control by design* governance framework). We hope the government does not miss this vital opportunity to produce a path-breaking statute, fit for the purpose of addressing the enormous risks posed by surveillance capitalism and the toxic business model it inspires and supports.

All of which is respectfully submitted,



Jim Balsillie  
Founder, Centre for Digital Rights

**Appendix A**  
**Other recommendations to strengthen Bill C-27**

**10.1 Hold directors and officers personally liable.**

The CPPA should hold directors and officers personally liable for AMPs or fines to promote good corporate governance and to help ensure corporations meet their legal obligations. Failing to do so will allow companies that commit serious CPPA violations to shut down following a significant AMP and/or fine and to reopen under a new corporate entity (this is especially problematic with smaller and more flexible entities). Personal liability for fines and imprisonment has proven to be an effective deterrent of bad behaviour by corporations under other Canadian federal and provincial legislation, including violations under CASL, workplace health and safety legislation, and environmental laws.

**10.2 Equip the Privacy Commissioner with the power to seek disgorgement of the organization's profits accruing from its unlawful activity under the CPPA.**

The CPPA should clearly prescribe a disgorgement remedy tied not to traceable economic injury but to violations of publicly-defined design, operational, and monitoring requirements.

## Appendix B

### Recommendations for further study

**11.1 Develop and implement a new and robust home-grown "control by design" governance framework to reset the old and failing "privacy by design and default" protections that were first developed in Canada in the 1990's, more recently gained prominence in privacy law reform in many jurisdictions (including Quebec and throughout the EU), but alone are now not fit for purpose and must be modernized.<sup>27</sup>**

#### *Reasons for control by design (CbD)*

Digital governance is the most important policy issue of our time. We have undergone, and continue to undergo, a digital transformation, resulting in a reliance on internet and telecommunications infrastructure for the open and rapid exchange of information. This transformation raises cross-cutting issues about values, the distribution of wealth, preserving competitive markets, preserving privacy, preserving health, maintaining the integrity of the democratic process, and ensuring national security.

Digital governance is about control. Whoever controls the data and the algorithms processing it, controls who and what interacts with it. Currently we do not control our own data. We "consent" to the collection and uses of our personal data in order to use a product or service and our data takes off for the Wild West. Any data collected can be algorithmically processed and analyzed in multiple ways that typically are not well understood by the data subject at the time of collection. This is the supply chain of data brokers and the data feed for surveillance capitalism.

The processing of data in ways that are new and unanticipated has major implications for security, democracy and the global economy. The current lack of personal and democratic control of data and algorithmic practices in the digital economy has led to increasingly widespread negative effects, on larger groups, particularity among vulnerable populations including children.

We must update our inadequate laws and institutions so that they are equipped to deal with the market power of those who wield data and algorithms at massive scale.

*Privacy by design and default* were well-intentioned privacy-enhancing innovations two decades ago (when most organizations treated privacy as an afterthought or did not think about privacy at all). While today there is still some scope for these tools to support a modicum of both privacy protection hygiene by organizations and control by individuals over their personal information (PI), privacy by design and default, in and of themselves, are wholly insufficient to address the structural asymmetries and the exploitative economic

---

<sup>27</sup> The January 2023 ISO Standard (ISO 31700-1) and Technical Report (ISO/TR 31700-2) documents respecting Privacy by Design were reviewed and determined not to require any adjustment to these recommendations.



logic at play in today's data-driven economy dominated by the toxic business model of surveillance capitalism.

That's because the "designer" is the organization. For example, even Facebook's privacy policy states that it designs privacy into their products from the outset. Its track record shows otherwise. A Facebook whistleblower detailed in the Wall Street Journal that Facebook already knows, in acute detail, that its platforms cause harm by design, often in ways only Facebook fully understands.

### *Nature of CbD*

In essence, CbD is a governance framework whereby democratically accountable powers (**DAPs**) or data stewards (such as data utilities reporting to government or data stewardship trusts with responsibilities to serve both data subjects and the public interest) control significant personal information datasets. CbD would impose a fiduciary responsibility on such stewards tantamount to the “do no harm” ethic of the Hippocratic Oath.

CbD is explicitly aligned with the espoused aims of Bill C-27, to implement the *Digital Charter* - most evidently in Principle 3 Control and Consent: *Canadians will have control over what data they are sharing, who is using their personal data and for what purposes, and know that their privacy is protected.*

CbD is a control-based approach to digital governance, establishing duties of care on data stewards to act in the interests of the owners of the personal data – Canadians themselves. The DAPs would also control who and what interacts with the data. An organization does not have to own data to control it. A DAP, with a fiduciary or fiduciary-like duty to an individual, would clearly not be able to authorize the use of data that would result or likely result in harm.

CbD could ignite innovation and competition in the tech sector, for example, DAPs could establish data pools or data trusts for the public good.

CbD is not a model where organizations continue to self-govern significant personal information data sets. It ends the reign of organizations paying "lip service" to PbD. It also strikes at the core of the toxic business model that surveillance capitalism inspires and supports.

If developed and implemented, CbD would constitute a made-in-Canada innovation of privacy laws and institutions that would restore Canada to its rightful place as a global pioneer in privacy protection.

## **11.2 Establish a fiduciary responsibility that imposes duties of loyalty and care on organizations that collect and use PI from individuals in circumstances of significant power and information imbalances or where individuals lack the ability to ensure compliance.**

This would be a natural and logical extension of fiduciary duties in Canadian law. Fiduciary duty cases in Canadian courts routinely deal with confidentiality issues. Fiduciary duties

arise from dependencies and power imbalances, in circumstances of trust and confidentiality. Clients and patients are dependent on their lawyers and physicians - professionals with privileges and powers in the legal and medical systems that clients and patients lack. They entrust their PI to their lawyers and doctors, who must maintain the PI's confidentiality, or face stiff penalties. Hence, lawyers and physicians have *per se* fiduciary duties.

It is no different with many organizations - e.g., social media platforms. As clients and patients do with their professionals, social media users entrust their PI to platforms, reasonably expecting a degree of confidentiality. Users surrender control over their PI, and so, are dependent on the platforms to use their powers to control and use it responsibly. Fiduciary duties would restrict self-dealing and reckless behaviour from those that collect, use and disclose PI in the function and design of their products and services. The greater the power and information imbalances between an individual and the organization, the more individuals are left vulnerable through exposure of their PI, and the higher the duty to which the trusted organization must be held. Children are an example of a group of vulnerable individuals, dependant on and entrusting of organizations to comply with their privacy obligations, but without the power to enforce or even monitor them.

American legal scholars are engaged in a debate over "Information Fiduciaries". Some view imposing fiduciary duties as necessary. Others view the prospect as problematic. Canadian fiduciary law is more expansive than that of the U.S. system. The American debate may thus have less resonance here. Also, the greater breadth of Canadian fiduciary principles make them more readily applicable to privacy. Such fiduciary responsibilities could be rooted in the CPPA (leaving space to grow by regulation) with a provision regarding an organization's duties of confidentiality and care when entrusted with PI, along the following lines (drawn from section 122 of the *Canada Business Corporations Act*):

#### **Fiduciary responsibility of organizations**

XX(1) Every organization in collecting, using or disclosing an individual's personal information, where there is a significant power or information imbalance between the organization and the individual, shall:

(a) be deemed to owe a fiduciary duty to act honestly and in good faith with a view to the best interests of the individual; and

(b) exercise the care, diligence and skill in the protection and use of the individual's personal information that a reasonably prudent organization would exercise in comparable circumstances for that purpose.

(2) When acting with a view to the best interests of the individual under paragraph (1)(a), the organization shall consider the following factors:

- (a) [list factors, each with a separate subparagraph]; and
- (b) such other factors as may be prescribed [i.e., by regulation.]

The terms "power imbalance" and "information imbalance" would be clearly defined in the statute. The essence of the definition is the imbalance that arises from individuals' lack of control over, or window on, the use and storage of their PI once it is surrendered to the organization. The PI is substantially or entirely within the organization's power, independent of the individuals. And in order to avoid an obvious loophole, the fiduciary duty would "travel with the data". In other words, if the organization is sold or merged, or if the organization's data set is transferred, the fiduciary duty covering the PI remains in place, and the new owner is bound by it to the same extent as its predecessor.

### **11.3 Provide the Office of the Privacy Commissioner with sufficient funding for it to properly fulfill its mandate.**

One approach worth considering for providing the OPC with a revenue stream commensurate with its mandate is to require all organizations covered by the CPPA to pay a modest annual fee dedicated to supporting the Office. This model also has the advantage of giving the Commissioner greater independence from the government of the day, as is appropriate for an Officer of Parliament. One way to implement such a revenue model is to base the fees on the number of individuals that the organization holds data on, as well as the sensitivity of the information handled. This would correspond to the Commissioner's compliance workload and holds intuitive appeal for individuals. Preliminary calculations suggest that an easily affordable *per capita* fee could greatly increase the OPC's budget. An added benefit of requiring all organizations covered by the CPPA to register is that it could bring greater transparency to the largely invisible data brokerage ecosystem. More details on this approach follow.

#### *Recommendation to further study "registration fees to support the OPC"*

While the privacy challenges of the data economy have exploded over the past decade, the capacity of the Office of the Privacy Commissioner to fulfill its mandate under PIPEDA has not grown proportionately. Effectively deploying its new CPPA powers further calls for significantly increasing the Commissioner's budget, as noted in the recent 2021-2022 Annual Report to Parliament. This is especially important for the OPC as it will be taking on the expected court challenges when it imposes AMPs on well-resourced violators. Unless the government is willing to commit to increasing its funding commensurate with the OPC's needs, additional sources of revenue will be necessary.

A clear indication that the OPC is not adequately resourced is that its annual budget barely grew over the period of 2010 to 2020, hovering around \$25M/yr.<sup>28</sup> It has increased in the past couple of years, to just under \$37M in the most recent budget available. With a Canadian population of over 38M, the federal government spends just under \$1 per person on average to enforce its privacy/data protection legislation across both public and private

---

28. Based on Net cash provided by Government in the OPC's annual reports. See latest report here.

sectors. By comparison, Facebook's US/Canada average annual revenue per user has risen exponentially over this 10-year period, from US\$3.20 to \$53.56 as of the 4<sup>th</sup> quarter of 2020.<sup>29</sup> In Canada, it costs an advertiser on average over US\$1 for a single user clicking on a Google ad.<sup>30</sup> The resource disparity between those who monetize personal information and those who protect it from abuse can hardly be more stark.

The UK's data protection public register offers an example and working model for Canada.<sup>31</sup> Its registration fees help make the Information Commissioner's Office one of the best funded in the world.

To see how a modest annual base registration fee based on the number of individuals and the sensitivity of their data could generate significant revenues for the OPC, consider this scenario.

Every organization would be required to report the number of individuals corresponding to each of these three categories:

- # of adults, for whom no sensitive information is handled;
- # of adults, for whom sensitive information is handled; and
- # of minors (whose data is inherently considered “sensitive”).

The annual registration fee could be calculated from a base rate per thousand individuals without sensitive data of \$10 per thousand, or 1 cent per person per year, with a surcharge when sensitive information is involved (e.g. double the base rate). Here is a sample of fees for a variety of hypothetical organizations:

Organization type	# of adults (no sensitive info)	# of adults (with sensitive info)	# of minors	Annual fee
Small retailer	2K	0	0	\$20.00
Mid-sized retailer	200K	0	0	\$2,000.00
Large bank	2M	0	100K	\$22,000.00
Large telco	1M	1M	0	\$30,000.00
Large data broker	1M	1M	1M	\$50,000.00

29. See Statista's chart: *Facebook's average revenue per user as of 4th quarter 2020, by region* here.

30. See Wordstream's *Average Cost per Click by Country* here.

31. Data Protection (Charges and Information) Regulations 2018 ss.2(2)-(3), 3 (the **Regulations**), as allowed under the Data Protection Act 2018 s.137.

Organization type	# of adults (no sensitive info)	# of adults (with sensitive info)	# of minors	Annual fee
Large social media company	0	10M	5M	\$300,000.00

Of course, the actual fee structure would need to be based on the OPC's funding needs and the data handling profile of the prospective registrants - i.e., the number of organizations and the scale of their data handling activities. This would very likely put the base rate for organizations at under one cent per data subject.

In an op-ed published in *The Globe and Mail*, Professor Andrew Clement looks at a "polluter pays" funding principle for Canadian privacy regulators.<sup>32</sup>

#### **11.4 Consider establishing a complaint funding mechanism to help finance legal proceedings brought by individual or group complainants and/or public interest organizations seeking remedies against organizations for alleged contraventions of the CPPA.**

The federal government, inspired by options currently under consideration in Europe and models already in place in Canada, should consider establishing a complaint funding mechanism (which could draw funds from the private sector, public sector, or both) to help finance complainants (i.e., individuals and groups and/or public interest organizations) seeking remedies against organizations for alleged contraventions of the CPPA. Such a pro-privacy-rights development has been the subject of a recent report by the European Consumer Organization (also known as the "BEUC") published in November 2022 entitled *Funding of Collective Redress – Financing options in the EU and beyond*. Canada could leverage the research and findings of this report to accelerate its thinking on the subject.

In addition and closer to home, the federal government could look to the Canadian Radio-television and Telecommunications Committee (CRTC) procedure for funding public interest participation with direct contributions from the private sector parties subject to the proceedings. Specifically, for many years now, the CRTC has had a procedure in place that allows public interest organizations who participate in CRTC telecommunications proceedings to apply for costs. In recently updated guidance (2022), the CRTC states that they often consider the active participation of organizations that represent consumer interests to provide a valuable contribution and recognize that these groups may require financial assistance in order to effectively participate in proceedings. As such, the CRTC may award costs to public interest organizations for their participation in telecommunications proceedings. Cost applicants must meet the threshold of contributing to "a better understanding of the matters that were considered", which takes into account the filing of evidence, whether the contribution was focussed and structured, and whether the contribution

<sup>32</sup> Clement, Andrew, "One way we could fund our privacy watchdog", *The Globe and Mail* (Ontario Edition), March 3, 2023.

offered a distinct point of view. It is the parties to a telecommunications proceeding, and not the CRTC, that pays the costs.

### **11.5 Protect the complainant's confidentiality and anonymity throughout the complaint process, including judicial reviews and appeals**

Nothing would be more ironic, but unfortunate, than for a Canadian to lose their privacy rights simply by making a privacy complaint or pursuing those rights in court. As a result, the CPPA should recognize the right for complainants to preserve, by default, their anonymity and confidentiality vis-à-vis the public. This right would apply not only in matters before the Privacy Commissioner (and the Personal Information and Data Protection Tribunal should the federal government retain the Tribunal, contrary to CDR's recommendation), but also in any court proceedings and filings related to the privacy complaint, including judicial reviews and appeals.

Specifying in the CPPA a right to anonymity and confidentiality in court proceedings is especially important. The "Open Court Principle" has privileged status in Canada. The Supreme Court has affirmed this repeatedly. As a result, court proceedings are presumptively open to the public.

The Supreme Court has equally recognized privacy to be an important public interest, and a quasi-constitutional right. The Court has emphasized the preeminent importance of an individual's ability to control the manner in which their personal information is collected, used and disclosed.

The Supreme Court has similarly ruled that the courts may make an exception to the Open Court Principle if a person's privacy is at serious risk.

By including in the CPPA the right by default to preserve anonymity and confidentiality in all proceedings, complainants will be spared the significant time, expense and stress needed to secure a sealing order to overcome the Open Court Principle. In today's digital world, the stakes for individuals and their personal privacy when decisions are published online are different and much higher thus supporting a broader discussion about privacy and the Open Court Principle.

Without such a right by default, there is a risk that potential complainants will be dissuaded from bringing forward issues to the Privacy Commissioner, for fear that their personal information could become publicly available. Consideration should therefore be given to whether this risk compromises the privacy process, and leaves it open to abuse, if private and confidential information in a matter before the Privacy Commissioner automatically became public when the matter moved to the courts. Such outcomes would seem to be at cross-purposes with the intent of the CPPA. Instead of promoting privacy, it could jeopardize the privacy of potential complainants.

The CPPA need not abandon the Open Court Principle entirely. Anonymity and confidentiality would be preserved by default, but the statute could offer an "opt out" provision. Complainants could waive the provision if they chose to be identified publicly. As well, the CPPA could allow a court or the Privacy Commissioner to order that a complainant's anonymity and confidentiality be removed, if there was proof of a compelling interest to do so (a sort of reverse sealing order).

## Appendix C

### Summary of over 40 recommendations (i) to fix Bill C-27's problems and make it fit for purpose, (ii) to strengthen Bill C-27, and (iii) for further study

#### **(i) Fixing and Making Fit Bill C-27**

- 1. Make Bill C-27 fit for addressing current privacy challenges and consistent with contemporary global privacy standards**
- 2. Frame the purposes of Bill C-27 properly**
  - 2.1. Recognize privacy as a fundamental human right
  - 2.2. Change the proposed legislation's name from "*Consumer Privacy Protection Act*" (CPPA) to "*Canada Personal Information Protection Act*" (CPIPA) or "*Canada Privacy Protection Act*" (CPPA)"
  - 2.3. Consult with Indigenous Peoples in modernizing Canadian privacy legislation including PIPEDA
- 3. Address the privacy risks to democracy**
  - 3.1. Expressly extend the CPPA to cover Canada's federal political parties
- 4. Recognize the serious privacy risks to groups as well as to individuals**
  - 4.1. Extend privacy protection to mitigate risks to groups
  - 4.2. Define "sensitive information" in keeping with the general principle of sensitivity set forth in section 12 of Quebec's Law 25 and the special categories of sensitive personal information (PI) enumerated in GDPR Article 9 (to ensure "adequacy") but on a non-exhaustive basis and with the addition of location-tracking information
  - 4.3. Protect minors with special, enhanced privacy requirements
  - 4.4. Clearly specify certain no-go zones as always being inappropriate purposes for collecting, using and/or disclosing an individual's PI
- 5. Fix the consent provisions**
  - 5.1. Strengthen valid consent in section 15 of the CPPA by restoring the "understanding" requirement in section 6.1 of PIPEDA
  - 5.2. Adopt a "legitimate interests" rule that clearly ranks the individual's interests and fundamental rights above the commercial interests of the organization in any assessment of the impact of relying on the rule

- 5.3. Eliminate implied consent as an alternative to the express consent basis for permitted collection, use or disclosure of PI
  - 5.4. Require separate, opt-in consent on digital media for collection, use or disclosure of personal information for purposes beyond what is necessary to provide a product or service
  - 5.5. Specify that the appropriate standard for determining the general impression to the average individual when ascertaining whether their consent has been obtained "deceptively" (and so is invalid) is the credulous and inexperienced person as opposed to the reasonable person
  - 5.6. Revise sections 15, 16 and 18 of the CPPA to address the concerns with the consent provisions raised in recommendations 5.1 through 5.5, above.
- 6. Use all the tools in the "privacy and consumer protection toolbox" to promote accountability**
- 6.1. Require organizations to conduct privacy impact assessments (PIAs) in advance of product or service development - particularly where invasive technologies and business models are being applied, where minors are involved, where sensitive PI is being collected, used, or disclosed, and when the processing is likely to result in a high risk to an individual's rights and freedoms
  - 6.2. Expressly require organizations to protect (i) privacy by "default" to align with Quebec's Law 25, section 9.1 and (ii) personal data by "design and default" to align with the GDPR, Article 25 (to help ensure "adequacy")
  - 6.3. Promote the development of data stewardship models
  - 6.4. Strengthen security safeguards
  - 6.5. Like Quebec's Law 25, the CPPA should have a separate section for cross border data flows requiring that organizations in Canada that export PI to a foreign jurisdiction for processing must first conduct a PIA to establish that the PI will receive an equivalent level of protection as in Canada.
  - 6.6. Adopt a more comprehensive regime governing third party data processors/service providers
  - 6.7. Clearly impose transparency and accountability obligations on data brokers.
- 7. Strengthen individuals' control over their PI**
- 7.1. Provide for a more comprehensive right to PI "mobility" (aka "portability")



- 7.2. Limit the exceptions to the right to "disposal" of PI (aka a right to "deletion"/"erasure"/"be forgotten") and provide for a right to disposal with respect to search engines' indexing of individuals' PI in specified circumstances
- 7.3. Strengthen information and access
- 7.4. Prohibit, subject to specific and narrow exceptions, organizations from using automated decision systems (ADS)/artificial intelligence (AI) to collect, use or disclose an individual's PI to align with GDPR, Article 22 (to help ensure "adequacy")
- 7.5. Give individuals the rights to contest and object to ADS/AI affecting them, not just a right to "algorithmic transparency"
- 7.6. Strengthen the private right of action
- 7.7. Adjust the CPPA's proposed regime for non-identifiable information (i) to make clear that organizations must apply appropriate processes to de-identify information and protect any such information and (ii) to provide that anonymized information complies with standards set out in regulations, to align with Quebec's Law 25

## **8. Give the Office of the Privacy Commissioner more teeth and bite**

- 8.1. Scrap the proposed Personal Information and Data Protection Tribunal
- 8.2. Provide for more flexible enforcement
- 8.3. Equip the Privacy Commissioner with the power to seek the imposition of administrative monetary penalties in a manner similar to the powers of the Commissioner of Competition under the *Competition Act*
- 8.4. Empower the Privacy Commissioner to issue "enforcement notices" and expand the sections for which the Privacy Commissioner can recommend penalties to include violations of the following: 12(1) (Appropriate purposes); 55 (3) (Disposal at individual's request: Reasons for refusal); 73 (Complaints and requests for information); 75 (Prohibition on re-identification); and 97 (Audits)
- 8.5. Strengthen the inter-agency collaboration and information-sharing provisions between the Privacy Commissioner, the Commissioner of Competition, and the CRTC
- 8.6. Strengthen the whistleblowing regime
- 8.7. Implement a self-reporting program for organizations

**9. The *Artificial Intelligence and Data Act (AIDA)* is foundationally flawed, needs proper consultation, and should be sent back to the drawing board (but don't leave it to ISED alone)**

- 9.1. AIDA is improper and incomplete
- 9.2. AIDA inappropriately focuses excessively on risks of harms to individuals to the exclusion of collective harms
- 9.3. AIDA possesses contradictory language and fragile enforcement powers
- 9.4. AIDA inappropriately focuses on an overly narrow range of algorithmic techniques
- 9.5. Go back to the drawing board on AIDA, but don't leave it to ISED alone

**(ii) Strengthening Bill C-27**

- 10.1 Hold directors and officers personally liable
- 10.2 Equip the Privacy Commissioner with the power to seek disgorgement of the organization's profits accruing from its unlawful activity under the CPPA

**(iii) For further study**

- 11.1 Develop and implement a new and robust home-grown "*control by design*" governance framework to reset the old and failing "*privacy by design and default*" protections that were first developed in Canada in the 1990's, more recently gained prominence in privacy law reform in many jurisdictions (including Quebec and throughout the EU), but alone are now not fit for purpose and must innovatively be modernized
- 11.2 Establish a fiduciary responsibility that imposes duties of loyalty and care on organizations that collect and use PI from individuals in circumstances of significant power and information imbalances or where individuals lack the ability to ensure compliance
- 11.3 Provide the Office of the Privacy Commissioner with sufficient funding for it to properly fulfill its mandate
- 11.4 Consider establishing a complaint funding mechanism to help finance legal proceedings brought by individual or group complainants and/or public interest organizations seeking remedies against organizations for alleged contraventions of the CPPA.
- 11.5 Protect the complainant's confidentiality and anonymity throughout the complaint process, including judicial reviews and appeals

## Appendix D

### Busting the myth that stricter privacy regulation stifles innovation

While it is often broadly claimed that stricter regulation penalizes innovators, the research that has sought to measure the relationship between regulation and innovation does not support such claims. In contrast to sweeping assertions of inescapable “stifling” effects, scholars support the position that privacy regulation may impact innovation, but such impact depends on the regulatory design. For example, Lev-Aretz and Strandburg’s nuanced and ground-breaking research led them to conclude that:

"across-the-board assertions about the stifling effects of information privacy regulation on innovation are simply wrong. Worse, they distract from difficult and important questions of regulatory design. ... [W]ell-designed privacy regulation has the potential to improve the extent to which the market produces a socially desirable portfolio of innovations."<sup>33</sup>

Goldfarb and Tucker’s research similarly suggests that privacy regulation may affect the extent and direction of data-based innovation, however, the impacts of privacy regulation can be extremely heterogeneous.<sup>34</sup> Further, Martin et al’s research, which examined how the introduction of the GDPR and enhanced data protection regulation affected start-up innovation in Germany, suggests that the effects of such privacy regulation are complex: it simultaneously stimulates and constrains innovation.<sup>35</sup> Aridor, Che and Salz’s research<sup>36</sup>, which examined the impact of the GDPR on an online travel intermediary, supports the position that regulation impacts businesses but does not necessarily stifle or harm business interests.<sup>37</sup>

CDR is strongly of the view that robust contextually appropriate<sup>38</sup> rigorous fairness, accountability and transparency rules for governing the flows of personal information do not stifle responsible innovation. They can do just the opposite. Instilling well-founded trust in individuals with respect to the potential innovative uses of their data, whether it be personally identifiable or anonymized, will only encourage responsible innovation.

---

<sup>33</sup> Yafit Lev-Aretz and Katherine J. Strandburg, *Privacy Regulation and Innovation Policy*, Yale Journal of Law and Technology (2020) 22:256, online: <https://yjolt.org/privacy-regulation-and-innovation-policy> at 263.

<sup>34</sup> Avi Goldfarb and Catherine E. Tucker, *Privacy and Innovation*, Innovation Policy and the Economy (2012) 12, online <https://doi.org/10.1086/663156>.

<sup>35</sup> Nicholas Martin et al, *How Data Protection Regulation Affects Startup Innovation*, Information Systems Frontiers (2019) 21:1307–1324, online <https://doi.org/10.1007/s10796-019-09974-2> (Nov. 18, 2019).

<sup>36</sup> Guy Aridor, Yeon-Koo Che and Tobias Salz, *The Economic Consequences of Data Privacy Regulation: Empirical Evidence from GDPR*, National Bureau of Economic Research (2020), online: <https://www.nber.org/papers/w26900> (Revised May 2021).

<sup>37</sup> In this case, the researchers found that enhanced privacy regulation initially led to a decline in revenue, but that over time such decline in revenue became smaller as the quality of the consumers that agreed to share information after the enactment of the GDPR increased and these consumers were determined to be more valuable than the pre-GDPR set of consumers.

<sup>38</sup> Nissenbaum, Helen. *Privacy in Context*, Stanford, California, Stanford University Press (2009).

In May 2021, the United Kingdom’s Taskforce on Innovation, Growth and Regulatory Reform (**UK Taskforce**)<sup>39</sup> published an independent report (the **TIGRR Report**)<sup>40</sup> concerning recommendations to the UK Prime Minister on how the UK could reshape its approach to regulation to drive innovation, growth and competitiveness. As a result of its consultation, the UK Taskforce recommended reform to UK privacy law to give stronger rights and powers to consumers and citizens, place proper responsibility on companies using data and free up data for innovation and in the public interest. The UK Taskforce maintained that regulation of the modern economy, including the digital economy, could encourage competition, stimulate innovation, and promote economic growth while concurrently protecting consumers and workers.<sup>41</sup>

The UK Taskforce noted that, in the context of developing and modernizing the UK’s regulatory framework, “regulation can be both an unnecessary barrier to growth for many businesses and a catalyst for investment in new sectors. Bad regulation is ineffective, expensive and difficult to implement. Good regulation, set up in the right way, can be a vital part of the infrastructure to support growth. Through setting clear, proportionate, long-term goals, frameworks and standards, UK regulation can be a significant driver of our international competitiveness.”<sup>42</sup>

Further, the UK Taskforce noted that a lack of regulation can in fact stifle innovation and investment. In its report, the UK Taskforce maintained that “the existence of a clear regulatory framework for a new sector is often a key precondition of investment”. In the UK Taskforce’s view, a lack of clarity and regulatory risk is holding back investment in certain areas like space, digital health, ‘mobility as a service’ and autonomous vehicles.<sup>43</sup>

The recommendations in the TIGRR Report indicate that regulating the modern digital economy requires a nuanced approach that focuses on proportionality of the risks associated with innovation and new technologies and the benefits gained, as well as the capacity of the organization being regulated. The UK Taskforce recommended that it is appropriate in certain instances to promote innovation through new standards and rules tailored specifically to SMEs and new market entrants<sup>44</sup> and it recognized that “care should be taken to avoid allowing large, established firms to shape regulation in their own interests where this comes at the expense of small competitors and potential market entrants”.<sup>45</sup>

CDR agrees with the UK Taskforce’s position that regulation, when thoughtfully crafted, can encourage and support innovation and enable SMEs and start-ups to compete with well-established players in the market.

---

<sup>39</sup> The UK Taskforce’s consultation included of a wide range of businesses, academics, think tanks through dozens of roundtables and meetings with over 125 experts on how the UK can improve how it regulates, now and in the future.

<sup>40</sup> Taskforce on Innovation, Growth and Regulatory Reform independent report, May 2021, online: [https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment\\_data/file/994125/FINAL\\_TIGRR\\_REPORT\\_\\_1\\_.pdf](https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/994125/FINAL_TIGRR_REPORT__1_.pdf)

<sup>41</sup> *Ibid.*, at 12.

<sup>42</sup> *Ibid.*, at 5.

<sup>43</sup> *Ibid.*, at 28.

<sup>44</sup> *Ibid.*, at 6.

<sup>45</sup> *Ibid.*

That said, a January 2022 working paper from the University of Oxford studied the economic consequences of the GDPR's introduction on firms targeting EU consumers.<sup>46</sup> It found that the GDPR's enhanced data protection measures and associated compliance costs caused an 8% decline in profitability.<sup>47</sup> The authors, however, caution their results for three reasons: (1) firms likely incurred one-time costs to comply with the new measures, decreasing profitability, (2) as the GDPR gradually becomes the global standard, firms targeting EU consumers will be less disadvantaged, and (3) the study does not account for aggregate welfare effects. Furthermore, the authors state "Though there is widespread concern that the GDPR has reduced digital innovation in Europe, it is equally plausible that it has accelerated innovation by inducing companies to develop new GDPR-compliant technologies".<sup>48</sup>

It is also worth noting that this working paper focussed on profitability, not innovation *per se*. As Lev-Aretz and Strandburg note, " 'Innovation' in [personal information]-based goods and services does not ... include improvements that result merely from employing "more" personal information in a known way, even if they increase market value." Innovation that earns public trust must involve novel information practices that benefit not just shareholders but society more generally. Carefully designed privacy regulations can help achieve this goal.

Furthermore, the "Brussels Effect" has been studied in the context of the GDPR. The "Brussels Effect", a term coined by Professor Anu Bradford, refers to the influence of regulation in the European Union outside of Europe, namely how multinational corporations elevate their regulatory standards and how EU standards become global standards.<sup>49</sup> The Brussels Effect was found to play a role in the adoption of the California Consumer Privacy Act (CCPA)<sup>50</sup> and is already having an impact on Canadian business in that some companies are processing EU data in a GDPR compliant manner. The CCPA and GDPR should align so that Canadians do not have a lesser set of rights.<sup>51</sup>

---

<sup>46</sup> Chinchih Chen, Carl Benedikt Frey, and Giorgio President, "Privacy Regulation and Firm Performance: Estimating the GDPR Effect Globally", (Oxford Martin School, University of Oxford, January 6, 2022), online: <https://www.oxfordmartin.ox.ac.uk/downloads/Privacy-Regulation-and-Firm-Performance-Giorgio-WP-Upload-2022-1.pdf>

<sup>47</sup> *Ibid* at 11.

<sup>48</sup> *Ibid* at 25-26.

<sup>49</sup> Bradford, Anu, "The Brussels Effect: How the European Union Rules the World" (2020). Columbia Law School *Faculty Books*. 232. Online: <https://scholarship.law.columbia.edu/books/232>

<sup>50</sup> Simon Gunst, Ferdi De Ville, "The Brussels Effect: How the GDPR Conquered Silicon Valley", *European Foreign Affairs Review*, Volume 26, Issue 3 (2021) pp. 437 – 458, online: <https://doi.org/10.54648/eerr2021036>; <https://kluwerlawonline.com/journalarticle/European+Foreign+Affairs+Review/26.3/EERR2021036>

<sup>51</sup> Bennett, Colin, "One set of privacy rights for Europeans, a lesser one for Canadians? Why the Canadian consumer privacy protection act and the EU's general data protection regulation should be in alignment", (May 20, 2021), online: <https://www.colinbennett.ca/canadian-privacy/one-set-of-privacy-rights-for-europeans-a-lesser-one-for-canadians-why-the-canadian-consumer-privacy-protection-act-and-the-eus-general-data-protection-regulation-should-be-in-alignment/>

**Appendix E**  
**CDR's critique of the CMA's Privacy Reports**



CENTRE FOR DIGITAL RIGHTS

---

March 7, 2023

**By Email:** [asimpson@thecma.ca](mailto:asimpson@thecma.ca)

Alison Simpson, President & CEO  
Canadian Marketing Association  
Toronto-Dominion Centre  
55 University Ave, Suite 603  
Toronto, ON M5J 2H7

**Re: Modernizing Canada's federal private sector privacy law**

Dear Ms. Simpson,

At the end of my January 9<sup>th</sup> meeting with the CMA's [Privacy and Data Committee](#), your colleague Sara Clodman invited the Centre for Digital Rights (CDR) to review and comment on the CMA's February 2022 and October 2022 reports<sup>1</sup> (the **CMA Privacy Reports**) on modernizing PIPEDA.<sup>2</sup> This letter is CDR's reply to that invitation.

**Summary**

In CDR's view, the foundation of the CMA Privacy Reports is fundamentally flawed as it often rests on outlier reports whose authors are rarely expert or independent<sup>3</sup>. The CMA draws on these reports to support overly-simplistic privacy law and policy prescriptions based on industry myths and leaps in logic that betray a misunderstanding of the almost five years of experience with modernized privacy law in Europe and an unfamiliarity with the rich modern expert literature on protecting privacy rights in the data driven economy.

---

<sup>1</sup> Canadian Marketing Association, *Canada's Privacy Law Priorities: Better Protections for Canadians + Innovation for Economic Growth*, October 2022, online: [https://thecma.ca/docs/default-source/default-document-library/report\\_privacy-law-priorities-2022.pdf](https://thecma.ca/docs/default-source/default-document-library/report_privacy-law-priorities-2022.pdf) and Canadian Marketing Association, *Privacy law pitfalls: Lessons learned from the European Union*, February 2022, online: [https://thecma.ca/docs/default-source/default-document-library/cma-2022-report-privacy-legislation-pitfalls.pdf?sfvrsn=ed54bdf4\\_6](https://thecma.ca/docs/default-source/default-document-library/cma-2022-report-privacy-legislation-pitfalls.pdf?sfvrsn=ed54bdf4_6) (**CMA Privacy Pitfalls Report**)

<sup>2</sup> *Personal Information Protection and Electronic Documents Act*, S.C. 2000, c. 5, as amended.

<sup>3</sup> For example, as discussed under "Privacy perplexity" (see below starting at page 8), to justify overlooking the well-documented and real-person biennial consumer-survey findings from the Office of the Privacy Commissioner, the CMA merely cites an American law student's undergraduate paper and the online scraping work of an opaque AI bot that several well-respected Canadian privacy experts lament has received "misplaced trust".

## Introduction

As CDR reads the CMA Privacy Reports, the CMA is calling for:

1. a "made-in-Canada" approach (specifically, not one that exists elsewhere in the world); and
2. a comprehensive law that is neither (a) akin to Europe's *General Data Protection Regulation (GDPR)* nor (b) aligned with Quebec's treatment of privacy as a human right and key aspects of Quebec's Bill 64/Law 25 (specifically, enhanced GDPR-inspired protections where personal information crosses borders).

You reiterated this call in your recent op-ed in *The Hill Times* entitled It's time to bring Canada's privacy law into the digital age, February 15, 2023.

As you know from our recent meeting, and for the reasons articulated in this letter, I strongly disagree with this call by the CMA. So too do many of the privacy experts that CDR consults including Professor Colin Bennett as set forth in his recent op-ed in the *CIGI Newsletter* entitled "Privacy is Like Yoga" - and Other Myths, February 8, 2023. Professor Bennett also recently published an op-ed in *The Hill Times*, entitled: Privacy czar's Home Depot investigation exposes weaknesses in Ottawa's new privacy bill, February 24, 2023. And Professor Andrew Clement published an opinion in *The Globe and Mail* entitled, One way we could fund our privacy watchdog, March 2, 2023.

That said, there seems to be at least one important point on which we might agree: Canada's private sector privacy law must soon be modernized. But just as important we must get this reform of PIPEDA right: the new statute must be fit for purpose.

Accordingly, CDR invites the CMA to reconsider its position from the lens of Canadian individuals and groups, and especially to support the position that privacy be recognized as a fundamental human right. Having reviewed the CMA Privacy Reports, CDR has concluded that the CMA's position on modernizing PIPEDA gives short shrift to the human and societal harms associated with mass online tracking, especially those affecting minors and other vulnerable groups. As stated by federal Privacy Commissioner Dufresne in a recent speech:

"Personal privacy is not a right we should have to surrender in the name of innovation or profit, or even in the name of public interest. In cases of conflict – and these will be rare – between privacy rights and private or public interests, privacy will prevail.

...

I look forward to providing my advice to Parliament on how [Bill C-27] should be further improved." <sup>4</sup> (emphasis added).

In this letter, CDR responds to the main critiques of modernized privacy legislation that underpin the CMA Privacy Reports – namely, that:

1. GDPR-like privacy compliance is (a) too expensive and burdensome and (b) stifles innovation; and
2. Canadian privacy regulation should not be overly complex.

### **Discussion**

#### ***Privacy law compliance is too expensive and burdensome***

The CMA Privacy Reports assert that GDPR-like privacy law compliance is too expensive and burdensome, cautioning Canadian legislators to avoid a privacy regime that comes with a high financial cost and regulatory burden for privacy compliance. Many of the CMA's arguments against the adoption of a GDPR-like law are related to financial costs, and especially the costs for small- and medium-sized enterprises (SMEs). The CMA cites third party reports that assert that SMEs are concerned over the costs of "regulation", which is a term that can capture a broad range of circumstances. It is unclear how much of this concern is attributed to regulation generally as opposed to specific concerns about the cost of new privacy regulation in Canada, where there is already provincial and federal privacy legislation in place.<sup>5</sup>

By contrast and informed by the results of independent expert research, CDR does not share the view that robust privacy regulation necessarily impedes innovation (see below, under "Robust privacy regulation and responsible innovation"). Rather, CDR agrees with the new federal Privacy Commissioner of Canada's recent statements that privacy can support innovation and competitiveness, rejecting the "false choice" between privacy and innovation.<sup>6</sup>

A modernized PIPEDA will naturally require an examination of an organization's personal information practices in order to ensure compliance with any new laws passed – whether it is a "made in Canada" or a GDPR-like solution. The vast cultural, technological, and societal shift that has occurred over the past two decades in Canada cannot be ignored. Viewing the cost of a modernized PIPEDA only through a financial lens is too narrow and, without consideration of the bigger context, misses the mark. Many laws with direct application to innovative industries have justifiably significant financial costs and regulatory requirements to administer (for example, laws relating to the safety of drugs and to the protection of the environment). However,

---

<sup>4</sup> OPC Canada, Speech by Privacy Commissioner of Canada, Philippe Dufresne, *A discussion on privacy: priorities, challenges and opportunities*, January 25, 2023, online: [https://www.priv.gc.ca/en/opc-news/speeches/2023/sp-d\\_20230125/](https://www.priv.gc.ca/en/opc-news/speeches/2023/sp-d_20230125/)

<sup>5</sup> See CMA Privacy Law Pitfalls Report at page 3.

<sup>6</sup> *Supra* note 3.



this does not mean that these laws are not essential in a free and democratic society, in which data is vital.

Nowadays, everyone's lives are highly digitized with minors being especially prone to datafication. From minors' sensitive medical records, educational records, sports registrations, summer camps, interactions between friends online, government registrations, comments on social media or online posts, gaming apps, online hobbies, online classrooms, to first bank accounts, the amount of digital personal data created about Canadian children and youth today is unprecedented. In CDR's view, all Canadians are entitled to the human right of privacy and that it *should* be a compliance cost to ensure that the sensitive information of minors and other vulnerable persons and groups are effectively protected at law. This is only augmented by the omnipresence of cyber data breaches and malicious actors threatening to expose the sensitive data of millions of people. Merely stating that the information of minors in Bill C-27 is "sensitive" is not enough.

In CDR's view, minors must be protected with specific and enhanced privacy requirements. The proposed *Consumer Privacy Protection Act (CPPA)* should contain measures to curtail the prevailing online surveillance and behavioural manipulation of minors practices of organizations. The CPPA should advance specific protections for children and youth such as defining rules for age-appropriate consent and providing for a comprehensive code of practice for organizations collecting, using or disclosing children's personal information (such as the UK's September 2020 *Children's Code* and the September 2022 *California Age-Appropriate Design Code Act*).

### ***Privacy regulators need sufficient funding***

While privacy commissioners in Canada have issued several guidance documents, and have dedicated units to business advisory services, CDR agrees with the CMA that privacy regulators require sufficient funding in order to effectively administer and enforce their mandates. In CDR's October 2022 [Statement on Bill C-27<sup>7</sup>](#) (**CDR's C-27 Statement**), CDR recommends that further study be conducted on how to ensure the Office of the Privacy Commissioner (**OPC**) has such sufficient funding.

CDR's C-27 Statement also recommends scrapping the proposed Personal Information and Data Protection Tribunal, which would be costly to implement and administer, especially considering that there is an existing regime in place at the OPC. No justification (privacy law innovation or otherwise) has been given for such a tribunal. Its assigned role and composition raise serious concerns (including unnecessary complexity, delay, and uncertainty for both individuals and organizations in the resolution of a complaint). Further, there is no privacy law regime in the world (including in the European Union, California, Utah, Colorado, Virginia and Connecticut, and the proposed *American Data Privacy and Protection Act*), that has established a tribunal like

---

<sup>7</sup> Centre for Digital Rights, Not Fit For Purpose – Canada Deserves Much Better, Centre for Digital Rights Statement on Bill C-27, October 28, 2022, online: <https://centrefordigitalrights.org/files/document/2022-11-13/257-013312.pdf>

---

the Tribunal being proposed under Bill C-27. Australia, which published a report on February 16, 2023 reviewing its *Privacy Act*, has also not called for a tribunal like the one under Bill C-27, and instead has proposed greater powers to the Privacy Commissioner and the courts.<sup>8</sup>

The proposed introduction of the Tribunal would also introduce unnecessary delay and complexity in the resolution of complaints. You may have seen the recent decision of the UK's First Tier Tribunal (**UK Tribunal**) concerning an Enforcement Notice issued by the UK Information Commissioner's Office (**ICO**).<sup>9</sup> Firstly, the Notice followed a two-year investigation by the ICO. After the investigation, it took an additional year for the UK Tribunal to schedule hearings, then around 2.5 years from the time of the Notice to the date of the UK Tribunal's decision. And the matter is still ongoing since the ICO must decide whether it will appeal the decision to the courts. It's indisputable that "justice too-long delayed is justice denied"- the proposed Personal Information and Data Protection Tribunal under Bill C-27 should be scrapped to avoid undue delays for Canadians exercising their rights to justice.

Lastly, CDR recognizes that the cost of compliance may also be higher for companies that are not already in compliance with PIPEDA, a statute currently with limited financial penalties for non-compliance. However, the costs of non-compliance can be much higher. There have been several cases in Europe and elsewhere where Big Tech companies have been heavily fined for privacy violations.

### *Charging to surf the internet?*

The CMA Privacy Pitfalls Report asserts that "[a]n additional impact—one that is just beginning to take shape in the online world—is that if consumers provide less personal information, companies are considering whether to introduce new charges or increase current prices to offset lost revenues."<sup>10</sup> This assertion reiterates the narrative (which many privacy experts call out as a myth) that privacy is an impediment or trade-off somehow to profit. It also directly opposes the federal Privacy Commissioner's position.<sup>11</sup>

There are many initiatives in the privacy and technology space, such as privacy-enhancing technologies (**PETs**)<sup>12</sup>, as well as codes and standards for privacy compliance in areas such as de-identification, and innovative methods for capturing express consent. Ideally, both marketing and privacy teams would work together to find innovative solutions where there is a legitimate

---

<sup>8</sup> Australian Government, Attorney-General's Department, "Privacy Act Review Report 2022", online: [https://www.ag.gov.au/sites/default/files/2023-02/privacy-act-review-report\\_0.pdf](https://www.ag.gov.au/sites/default/files/2023-02/privacy-act-review-report_0.pdf)

<sup>9</sup> See <https://ico.org.uk/about-the-ico/media-centre/news-and-blogs/2023/02/tribunal-rules-on-experian-appeal-against-ico-action/>

<sup>10</sup> See CMA Privacy Law Pitfalls Report at page 18.

<sup>11</sup> *Supra* note 3.

<sup>12</sup> OPC Privacy Tech-Know blog: *Privacy Enhancing Technologies for Businesses*, (12 April 2021), online: <https://www.priv.gc.ca/en/blog/20210412/>

need to collect and use consumer data, since the viewpoint of the consumer concerns both privacy and marketing. The two do not necessarily require a trade-off.

Furthermore, in CDR's view some data practices are inappropriate. CDR's C-27 Statement submits that the CPPA should be amended to clearly specify certain no-go zones as always being inappropriate purposes for collecting, using and/or disclosing an individual's personal information. These inappropriate purposes and prohibitions should include (1) psychographic micro-profiling and micro-targeting for purposes of persuasion or influencing behaviour and (2) capturing biometric data without express consent (e.g., facial image scraping from websites, platforms and other locations on the internet).

### ***Robust privacy regulation and responsible innovation***

In its two papers, the CMA asserts that GDPR-like privacy regulation will have a stifling effect on innovation. On its face, this assertion has a superficial intuitive appeal. The North American Adtech business is unlikely to have grown to hundreds of billions of dollars annually if data protection regulation had not been so permissive. But in CDR's view it is now clear that much of this innovation has brought high costs to individuals and society more generally. Hopefully, the CMA can recognize this and is only interested in promoting responsible innovation – new forms of socio-economic value creation that bring widespread benefits.

Even taking this more restricted view of innovation, the CMA's assertion is at odds with the consensus of most independent privacy experts who have studied its economic implications. Moreover, when CDR reviewed the support for the proposition that robust privacy regulation decreases innovation, it found the sources relied upon by the CMA were overly narrow, limited to self-interested industry groups, and, in most instances, not held to the higher standards of peer-reviewed academic research publications.

For example, in the CMA Privacy Pitfalls Report under, "Hampering the ability of organizations to innovate and contribute to economic growth", there are numerous footnotes citing sources related to the financial costs of GDPR compliance and the GDPR impact on data transfers (see bottom of pages 10, 11, 12 and 13). However, CDR could not find sources to academic articles or independent research to support the position that GDPR-like privacy regulation would decrease innovation in Canada. Also, this CMA report cites three German industry sources: two from Bitkom<sup>13</sup>, which represents companies in the digital media space/digital economy<sup>14</sup> and another from the German marketing association, DDV.<sup>15</sup> CDR asks the CMA to point it to reports of experts independent from industry (and so not captured by corporate stakeholders with

---

<sup>13</sup> Datenschutz setzt Unternehmen unter Dauerdruck, Bitkom, 2021., online:

<https://www.bitkom.org/Presse/Presseinformation/Datenschutz-setzt-Unternehmen-unter-Dauerdruck>

Susanne Dehmel, Datenschutz als Daueraufgabe für die Wirtschaft: DS-GVO & internationale Datentransfers, Bitkom, 2021., online: <https://www.bitkom.org/sites/default/files/2021-09/bitkom-charts-pk-datenschutz-15-09-2021.pdf>

<sup>14</sup> <https://www.bitkom.org/EN/About-us/About-us.html>

<sup>15</sup> <https://nextcloud.ddv.de/index.php/s/Cb5JZ7fsHi2rieT>

---

a long history of opposing privacy law modernization) that support the claim that GDPR-like privacy regulation would decrease innovation in Canada.

CDR's C-27 Statement includes an Appendix D, entitled: "*Busting the myth that stricter privacy regulation stifles innovation*". CDR reviewed many scholarly articles and a government-commissioned advisory report that addressed the economic implications of data protection measures. CDR could find no evidence in these articles that GDPR-like privacy regulation would stifle innovation in Canada. Organizational behavior is influenced by many factors, only one of which is data protection. It is also worth noting that there are empirical studies on the effects of the GDPR on innovation in Europe, which claim a positive effect.<sup>16</sup>

The unsubstantiated assertion that robust privacy law (like the GDPR) negatively impacts innovation is dangerous in that it falsely implies privacy is a trade-off and an impediment instead of a fundamental human right, with inherent value, and something to be duly considered as such. For example, it can be innovative to create new video games apps, used by minors, that in turn, advertise other gaming apps based on an analysis of the use of those apps. However, it is predatory to advertise to minors in a manner using dark patterns, recognizing how susceptible children are to marketing. Such a practice is not responsible innovation, it's inappropriate manipulation.

To be considered "responsible", innovation needs to be assessed in more than simply economic terms and include wider public goods. In its C-27 Statement, CDR contends that the CPPA should expressly recognize privacy as a fundamental human right that is inextricably linked to other fundamental rights and freedoms including the rights to life and liberty (personal autonomy and self-determination), freedom of thought and expression, freedom from discrimination, and freedom from unjustified intrusion or surveillance. Such recognition should be made in both a new preamble to the CPPA itself (note that the current preamble, which arguably only applies to Bill C-27 overall, does not contain such recognition) and section 5 (Purpose) of the CPPA in order to provide clear guidance to those interpreting the CPPA. The addition of a reference to privacy as a fundamental human right in the preamble of the CPPA alone may be insufficient; to avoid any doubt, specific inclusion is needed in the body of the CPPA to give unambiguous legal effect to Parliament's intention that privacy be recognized as a fundamental human right.

In Europe, privacy and data protection are fundamental rights. The right to privacy is found in both the United Nation's *Universal Declaration of Human Rights* and the *International Covenant on Civil and Political Rights* (ICCPR). The Office of the United Nations High Commissioner for Human Rights recently issued a report in support of the right to privacy in the digital age.<sup>17</sup> CDR cannot understand why the CMA would push back on the position to adopt privacy as a human right in Canada and CDR encourages the CMA to reconsider its position. Under the GDPR,

---

<sup>16</sup> Niebel, Crispin, "The impact of the general data protection regulation on innovation and the global political economy", *Computer Law & Security Review*, Volume 40, April 2021, online (behind paywall): <https://www.sciencedirect.com/science/article/abs/pii/S026736492030128X>

<sup>17</sup> United Nations, General Assembly, Human Rights Council, Report of the Office of the United Nations High Commissioner for Human Rights, "The right to privacy in the digital age", August 2022 online: <https://documents-dds-ny.un.org/doc/UNDOC/GEN/G22/442/29/PDF/G2244229.pdf?OpenElement>

while privacy and data protection are fundamental rights, they can still be justifiably limited when it is both necessary and proportional. For example, the European Data Protection Supervisor (**EDPS**) has stated:

Necessity shall be justified on the basis of objective evidence and is the first step before assessing the proportionality of the limitation. ...proportionality requires that advantages due to limiting the right are not outweighed by the disadvantages to exercise the right. In other words, the limitation on the right must be justified. Safeguards accompanying a measure can support the justification of a measure. A pre-condition is that the measure is adequate to achieve the envisaged objective. In addition, when assessing the processing of personal data, proportionality requires that only that personal data which is adequate and relevant for the purposes of the processing is collected and processed."<sup>18</sup>

The regulatory model by which privacy is a fundamental human right gives individuals the right to control their personal information and its processing – especially in the context of automated decision systems/artificial intelligence, where risks to fundamental rights (such as the right to be free from discrimination and arbitrary decisions) are heightened.

Lastly, the OPC published an opinion by Addario Law Group LLP on March 31, 2022 indicating that a human rights-based approach to data protection is constitutional.<sup>19</sup>

### **Privacy perplexity**

The CMA Privacy Law Pitfalls Report relies heavily on a paper by a Member of European Parliament (**MEP**) Axel Voss to support the apparent problems arising from the alleged complexity of the GDPR.<sup>20</sup> However, in research that cites MEP Voss, there is also evidence that "acknowledging the difficulties of implementing the GDPR framework is not an endorsement of either watering down existing rules or taking an entirely different approach."<sup>21</sup>

The CMA's Privacy Law Pitfalls Report also cites the paper entitled, "*Hey Alexa, Do Consumers Really Want More Data Privacy?*" (written by Katherine Wilcox when she was in law school<sup>22</sup>)

---

<sup>18</sup> EDPS, online: [https://edps.europa.eu/data-protection/our-work/subjects/necessity-proportionality\\_en](https://edps.europa.eu/data-protection/our-work/subjects/necessity-proportionality_en)

<sup>19</sup> Addario, Frank and Samara Selter, Addario Law Group LLP, "Opinion Prepared for the Office of the Privacy Commissioner of Canada: The Constitutional Validity of Bill C-11, the Digital Charter Implementation Act", (*Office of the Privacy Commissioner of Canada*, March 31, 2022), online: [https://www.priv.gc.ca/en/opc-news/news-and-announcements/2022/op-c11\\_addario/](https://www.priv.gc.ca/en/opc-news/news-and-announcements/2022/op-c11_addario/)

<sup>20</sup> Voss, Axel, *Fixing the GDPR: Towards Version 2.0*, 25 May 2021, online: <https://www.axel-voss-europa.de/wp-content/uploads/2021/05/GDPR-2.0-ENG.pdf>

<sup>21</sup> Pam Dixon, Ugonma Nwankwo, and Michael Pisa, Centre for Global Development, *Why Data Protection Matters for Development: The Case for Strengthening Inclusion and Regulatory Capacity*, online: <https://www.cgdev.org/publication/why-data-protection-matters-development-case-strengthening-inclusion-and>, Page 5

<sup>22</sup> After graduating from Brooklyn Law School in 2020, Ms. Wilcox worked briefly as an associate lawyer at a US law firm before becoming in-house counsel at Epic Games in November 2022 (which was recently the subject of a major enforcement action by the US Federal Trade Commission: [Fortnite video game maker Epic Games to pay more](#)

to support that the GDPR is creating complexity for consumers.<sup>23</sup> The article itself states, "rather than parsing through ninety-nine articles and over 200 pages of complex regulatory text, this argument is supported primarily through case studies of major international tech companies focusing on how they collect and utilize user data."<sup>24</sup> Moreover, this American article does not seem to reflect the Canadian experience, as the OPC's most recent 2020-21 Survey of Canadians on Privacy Related Issues (OPC Survey), states:

"Nearly nine in 10 Canadians express some level of concern about protecting personal privacy.

...

Canadians are concerned about how their online personal information will be used by organizations.

...

Canadians are more likely to feel uninformed about how their personal information is handled by businesses and government, and many feel they have little control over how their information is used."<sup>25</sup>

The CMA also refers to a recent survey of Canadians conducted by an AI bot "Polly" and asserts that Canadians are twice as concerned about cybersecurity compared with data privacy and of those Canadians expressing concerns about data privacy, concerns about public sector use of personal information far outweigh concerns about commercial use. While certain of Polly's analysis aligns with the OPC Survey, caution has also been raised to consider whether AI bots like "Polly" have received misplaced trust.<sup>26</sup> Moreover, certain key findings of the most recent OPC Survey directly contradict the main conclusions reached by Polly – specifically, that under the OPC Survey: (1) Canadians are only marginally more concerned about security than privacy; and (2) Canadian concerns about public sector use of personal information do not outweigh concerns about private sector use.<sup>27</sup>

than half a billion dollars (US) over FTC allegations of privacy violations and unwanted charges, December 19, 2022). The Brooklyn Law Journal is a student-edited journal that accepts unsolicited manuscripts including those written by its students. All to say, Ms. Wilcox's paper may be "research and commentary" but it is neither expert nor peer-reviewed scholarship.

<sup>23</sup> Wilcox, Katherine M., *Hey Alexa, Do Consumers Really Want More Data Privacy?: An Analysis of the Negative Effects of the General Data Protection Regulation*, Brooklyn Law Review, 2019., online:

<https://brooklynworks.brooklaw.edu/cgi/viewcontent.cgi?article=2227&context=blr>

<sup>24</sup> *Ibid*, page 260.

<sup>25</sup> Office of the Privacy Commissioner of Canada, "2020-21 Survey of Canadians on Privacy Related Issues", (March, 2021), online: [https://www.priv.gc.ca/en/opc-actions-and-decisions/research/explore-privacy-research/2021/por\\_2020-21\\_ca/](https://www.priv.gc.ca/en/opc-actions-and-decisions/research/explore-privacy-research/2021/por_2020-21_ca/)

<sup>26</sup> Dubois, Elizabeth, *Federal election 2021: Why we shouldn't always trust 'good' political bots*, September 19, 2021, online: <https://theconversation.com/federal-election-2021-why-we-shouldnt-always-trust-good-political-bots-168137>

<sup>27</sup> This biennial survey commissioned by the Privacy Commissioner of Canada and conducted by Phoenix Strategic Perspectives Inc. seeks to better understand the extent to which Canadians are aware of, understand and perceive privacy-related issues. The survey notes that Canadians are only marginally more concerned about security than privacy (89% to 87%). Further, it finds that Canadians' concerns about public sector use of personal information (PI) do not outweigh concerns about private sector use of PI. Canadians feel slightly more informed about how their

The CMA also cites a Global Data and Marketing Alliance (GDMA) 2022 report entitled "*Global Data Privacy: What the Consumer Really Thinks*"<sup>28</sup> and asserts that more Canadians are "Data Pragmatists", as opposed to "Data Fundamentalists" or "Data Unconcerned". These segmentation categories are outdated, tracing back to Professor Alan Westin's privacy segmentation model. Recent scholarship has questioned this segmentation model, stating it is structurally flawed and over cited:

Alan Westin's well-known and often-used privacy segmentation fails to describe privacy markets or consumer choices accurately. The segmentation divides survey respondents into "privacy fundamentalists," "privacy pragmatists," and the "privacy unconcerned." It describes the average consumer as a "privacy pragmatist" who influences market offerings by weighing the costs and benefits of services and making choices consistent with his or her privacy preferences. Yet, Westin's segmentation methods cannot establish that users are pragmatic in theory or in practice.<sup>29</sup>

Significantly, the same GDMA report finds that consumers would like to have more control over their personal information, continue to seek transparency as a precursor to sharing that information and have growing expectations of industry to protect their information.<sup>30</sup>

Also, the GDMA report finds that among Europeans there is a significant growth in awareness of the GDPR, helping to encourage a growing confidence in data sharing:

"Despite the variations across markets and age groups, there has been a clear and significant rise in public awareness of GDPR in European markets. Such findings suggest that a growing understanding of regulatory protections has helped encourage and nurture the growing sense of comfort and confidence with data sharing...."<sup>31</sup>

Clearly, notwithstanding the recognized challenges in achieving implementation of the GDPR, its adoption has led to an increased sense of confidence among European consumers regarding the uses of their personal information by organizations – a testament to the validity of the GDPR's data protection regime. Far from being perplexed by the GDPR's regime, Europeans are looking to it as a beacon for protecting their personal information in the evolving global data ecosystem. Furthermore, the effects of the GDPR are already being seen beyond Europe as many companies operating in Canada are already forced to comply with its terms. Companies are already trading up to this standard, why should Canada continue to lag behind?

---

PI is handled by the public-sector (a 3% difference) and are far more confident that the federal government respects their privacy rights compared to private businesses (an 18% difference).

<sup>28</sup> <https://globaldma.com/wp-content/uploads/2022/03/GDMA-Global-Data-Privacy-2022.pdf>

<sup>29</sup> Urban, Jennifer M. & Chris Jay Hoofnagle, "The Privacy Pragmatic as Privacy Vulnerable", (*CUPS, Carnegie Mellon University Security and Privacy Institute*, 2014), online: <<https://cups.cs.cmu.edu/soups/2014/workshops/privacy/s1p2.pdf>> .

<sup>30</sup> Executive Summary, GDMA report.

<sup>31</sup> GDMA report at pp. 31-32.



***PIPEDA's purpose clause is outdated***

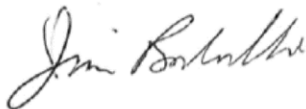
CDR does not agree with the CMA that PIPEDA's purpose clause is a "widely recognized strength", since it lacks the recognition of privacy as a human right, despite the numerous global instruments which find otherwise. Privacy is recognized as a human right in Quebec, under the Council of Europe's Convention 108+, in the GDPR, and in a growing number of countries such as Brazil and South Korea. Moreover, both the last Canadian privacy commissioner (Daniel Therrien) and the current Canadian privacy commissioner (Philippe Dufresne) are on the public record stating their respective strongly-held beliefs that privacy is a fundamental right.<sup>32</sup>

To quote the Canadian Human Rights Commission: "Human rights describe how we instinctively expect to be treated as persons . . . You do not have to earn your human rights. You are born with them."<sup>33</sup> Numerous countries/jurisdictions throughout the world recognize privacy and/or data protection as a fundamental human right. In CDR's view, the CPPA continues to prioritize business interests over the individual, by continuing to normalize surveillance capitalism and failing to make privacy a fundamental human right.

\*\*\*

CDR appreciates the CMA inviting feedback from CDR on the CMA Privacy Reports and encouraging debate with the aim of achieving a robust federal private sector privacy framework in Canada. CDR hopes the CMA will review CDR's C-27 Statement and consider supporting the recognition of privacy as a fundamental human right, a step forward for ensuring a better digital future for all Canadians and especially those who require greater protections, such as minors.

Sincerely,



Jim Balsillie  
Founder, Centre for Digital Rights

cc: Sara Clodman, Vice-President, Public Affairs and Thought Leadership, CMA

---

<sup>32</sup> *Supra note 3*; Office of the Privacy Commissioner of Canada, *Submission on Bill C-11, the Digital Charter Implementation Act, 2020*, May 2021, online:

[https://www.priv.gc.ca/en/opc-actions-and-decisions/submissions-to-consultations/sub\\_ethi\\_c11\\_2105/](https://www.priv.gc.ca/en/opc-actions-and-decisions/submissions-to-consultations/sub_ethi_c11_2105/)

<sup>33</sup> Canadian Human Rights Commission, *What Are Human Rights?*, online: <https://www.chrc-ccdp.gc.ca/en/about-human-rights/what-are-human-rights>, accessed Feb 2023.



**Appendix F**  
**CDR's Critique of the ISED's Companion Document for AIDA**

**What ISED's "Companion Document" Teaches Us:  
No AIDA would be better than this AIDA**

**Introduction**

The AIDA “Companion Document” (CD) that ISED published on March 13, 2023 does not advance AIDA’s case. It is unadvisable to rely on the document for decisions concerning AIDA. AIDA is slapdash, undemocratic draft legislation. Cobbled together in haste, AIDA omits crucial protections for Canadians, and ignores key aspects of AI regulation needed to align Canada with the EU.

The CD is untrustworthy due to its rushed construction. It makes clear that (i) AIDA will not (adequately) protect Canadians collectively and individually, and (ii) AIDA will diminish Canada as a player in the global tech world. The CD shows up AIDA for being so flawed that sending AIDA back for a rewrite would be safer than relying on this draft, even with amendments.

Simplifying, the CD highlights failings in AIDA that fall into three broad categories:

1. It leaves Canadians exposed to multiple harms.
2. It is profoundly undemocratic.
3. It is a setback to Canada’s place on technology’s international stage.

**1. Leaving Canadians Exposed to Harms**

There are widespread, well-founded concerns that if not properly regulated, AI developments run serious risks of harm - to individuals, communities and society more generally. Prominent public figures, AI researchers, government officials, civil society organizations and lay individuals have each expressed deep concerns that if not checked, AI applications threaten many aspects of contemporary life.

AIDA fails to protect individuals and groups of individuals from the destructiveness of which these multiple stakeholders warn. The CD merely glosses over the potential harms.

Even if we ignore the adverse effects of AI that have yet to emerge, AIDA leaves Canadians prey to a multitude of dangers that the CD overlooks. This is only an incomplete list: job loss, behaviour manipulation, mental health disturbance, economic deprivation, labour exploitation, security degradation, autonomous weapon implementation, 'deepfakes' and mis-information, public resource misallocation, public safety threats, and erosion of democracy.

These risks are not hypothetical. Advocates, researchers, and everyday users of technology have documented them.

The CD makes no attempt to address the harms comprehensively. It captures a few of them, in part, when it refers to “systems of interest”, or offers the very limited examples of gender or

racial discrimination, and deepfake images, audio and video “that can cause harm to individuals”.

But these sample harms are selective. They focus on individuals not society. The CD is silent, for example, on the realistic prospect of Big Tech using AI to entrench their global surveillance capitalism business model even more deeply. Potential harms to public safety from 'weaponized' AI systems that the government knows about are also oddly missing and apparently out of AIDA's scope.

Even more surprising is that the CD says nothing about the threats that AI-based systems pose to elections in Canada and democracy generally.

How could the CD be so constricted in scope? Sloppiness due to hasty preparation? Or was it to bolster an intentionally rigid policy preference to focus only on the most overt individual harms, and avoid addressing the multitude of societal AI threats? The latter interpretation is consistent with AIDA's overall language, which skews to individuals at the expense of society more broadly.

Other omissions in the CD: harms in the development of AI systems, not just their use or output; mental health harms, in addition to quantifiable, material ones; and environmental damage, the concern of all.

The CD and AIDA itself must address the many forms of collective harms broadly, and not limit itself to quantifiable individual harms narrowly.

## **2. Profoundly Undemocratic**

The CD underscores just how profoundly AIDA erodes Canadian democratic norms in two ways: first, by deviating from proper public consultation, and second by combining both regulatory oversight and promotion functions concerning AI in one body: ISED. A textbook conflict of interest.

### **No Proper Consultation**

AIDA first appeared in June 2022 as Part III of Bill C-27. There was no prior notice. There were no public hearings. The CD's silence on this short-circuiting of the transparent legislative process fundamental to democracy in Canada is curious.

Lawmaking without public consultation breeds mistrust amongst Canadians, especially with complex subject matter as sensitive as AI. The CD does nothing to address this worry. Suspicions around technology and big tech companies run high already. How can Parliament expect Canadians to trust (or respect) AIDA when it has denied them the normal participation in its creation?

The very characteristics of AI that make a proper legislative process imperative — novelty, complexity, breakneck expansion into varied facets of modern life – make jettisoning public

consultation even more dangerous. The CD must give guidance on securing multiple perspectives on the core issues Parliament must resolve to dispel confusion: clarify what AI actually is; tame hyperbole about AI's perils and promises; and counter the messaging from powerful actors racing to dominate the field.

### **Conflict of Interest**

AIDA relies on the same Department for both regulatory oversight, and for promoting and supporting AI in Canada. The CD goes to some lengths to avoid describing ISED's dual role for what it is: a conflict of interest.

The CD explains away the conflict by speaking of "the unique AI regulatory context," and asserting that oversight and encouraging innovation need to "work in close collaboration in the early years of the framework under the direction of the Minister". This statement is disingenuous, since it cites the OECD's Best Practice Principles for Regulatory Policy as justification for the Minister's double role when the OECD explicitly recommends just the opposite - that "this combination should be avoided".

Deviating from good governance principles at the start is hardly a sound basis for creating a reliable regulatory regime in the public interest. It would take much more than the CD's assertion that "AI is unique" to justify ISED's conflict of interest and earn Canadians' trust in AIDA, especially after it bypassed the normal public consultation process.

The absence of substantive detail in the CD invites the suspicion that the Minister is protecting his prerogatives and the industry he promotes. This does not bode well for AIDA's future.

### **3. International Setback**

The CD rightly describes Canada as "a world leader in the field of artificial intelligence". It wrongly implies that AIDA is aligned with EU, OECD and other international AI norms. As proposed, AIDA pulls Canada back from its AI leadership role.

First, ISED's conflict of interest (above) violates OECD norms. The OECD says that assigning both industry development and regulatory functions to one body reduces the regulator's effectiveness in one or both functions, and also fails to engender public confidence. Second, AIDA confines its definition of an "artificial intelligence system" to a much narrower set of algorithmic techniques than the EU's draft AI Act. AIDA applies only to "high impact" AI.

The EU AI Act, however, explicitly covers a broad range of low to high risk algorithmic techniques. The amendments to the EU AI Act explicitly define "artificial intelligence system", "risk", "significant risk", "foundation model", "general purpose AI system" and "large training models."<sup>52</sup> By comparison to the EU's draft law, AIDA misses many potential harms, such as divisive or politically manipulative messaging which may not depend on the small set of novel

---

<sup>52</sup> See EU AI Act, consolidated text, 11 May 2023, online: [https://www.europarl.europa.eu/meetdocs/2014\\_2019/plmrep/COMMITTEES/CJ40/DV/2023/05-11/ConsolidatedCA\\_IMCOLIBE\\_AI\\_ACT\\_EN.pdf](https://www.europarl.europa.eu/meetdocs/2014_2019/plmrep/COMMITTEES/CJ40/DV/2023/05-11/ConsolidatedCA_IMCOLIBE_AI_ACT_EN.pdf)

techniques that AIDA lists in its definition of AI. These few techniques far from exhaust the many longstanding “high-impact” algorithmic practices readily available to malicious or irresponsible actors.

Finally, AIDA’s focus on individual rather than collective harms puts it at odds with the AI Risk Management Framework from the U.S. National Institute of Standards and Technology (NIST). Page 1 of the NIST document notes that AI technologies “pose risks that can negatively impact individuals, groups, organizations, communities, society, the environment and the planet”. The CD simply ignores the broader harms, creating unwanted distance between American and Canadian approaches to AI.

The CD avoids the hard truth that AIDA’s definitions are clearly at odds with those of the OECD, the EU and the U.S. This non-conformity risks a practical misalignment that could thwart Canada’s ambition to preserve and grow our data economy’s interoperability in international markets.

## Conclusion

While the CD is helpful in clarifying some of the Government’s intentions in some areas concerning AIDA, it falls well short of giving the guidance that Parliamentarians need before voting on such an important new law.

The CD’s abundant weaknesses and lack of relevant substance deepen concerns that (i) the Government has not conducted due diligence in drafting the legislation, (ii) lacks a viable plan, and (iii) is engaging in a public relations exercise. This compels the conclusion that, even with optimistic assumptions about the Government’s willingness to adopt amendments in Committee, they are unlikely to fix AIDA’s fundamental flaws in process and substance.

AIDA and the CD should be sent back to be drafted anew, but not by ISED alone. Such a reset would enable robust public consultation and the active participation of the relevant government departments and commissions that were passed over in the initial drafting. Both are vital to crafting good laws. And given that the CD anticipates AIDA not coming into full force until at least 2025, an earnest and democratic drafting effort starting now would not significantly delay bringing a good AI law into effect.

In addition, Canadian lawmakers should consider whether (if only as a transitional interim measure to address key regulatory gaps) there are any lessons in the United Kingdom’s March 28, 2023 proposal for AI governance, A pro-innovative approach to AI regulation, to leverage.<sup>53</sup> Specifically, this UK whitepaper proposes self-styled “agile regulation” whereby five principles for responsible AI development and use<sup>54</sup> are set out and existing regulators (such as privacy and

---

<sup>53</sup> See, for example, Teresa Scassa, Comparing the UK’s proposal for AI governance to Canada’s AI bill, April 11, 2023.

<sup>54</sup> These principles are (1) safety, security and robustness, (2) appropriate transparency and explainability, (3) fairness, (4) accountability and governance, and (5) contestability and redress.

competition authorities) and being both specifically directed and further enabled to regulate AI according to these principles within their areas of responsibility.

A fresh start would better lead to a law that earned Canadians' trust and maintained Canada's place on the world AI stage, instead of one that called loudly for immediate repair. A flexible law on sound foundations is better than an ill-founded hasty law, especially in the rapidly changing AI arena, fraught with promise, peril and uncertainty.

## Appendix G

### CDR's critique of the federal government's amendment to the *Canada Elections Act* as part of Bill C-47 (the 2023 Budget legislation) purporting to implement a "national, uniform, exclusive and complete regime" for the FPPs' protection of Canadians' privacy

Buried in the back pages of the 270 page long federal Budget 2023 published on March 28, 2023 was a proposal that Canada's federal political parties (FPPs) should be subject to a "uniform approach" to privacy protection under the *Canada Elections Act* – specifically

In Budget 2023, the government proposes to amend the *Canada Elections Act* to establish a uniform federal approach in respect of federal political parties' collection, use, and disclosure of personal information in a manner that overrides overlapping provincial legislation.

On April 20, 2023 and to implement Budget 2023, the Government introduced Bill C-47 which received Royal Assent on June 22, 2023 and included the following amendments to the *Canada Elections Act* (now in force as section 385.2):

680. The *Canada Elections Act* is amended by adding the following after section 385.1:

#### Definition of *personal information*

385.2(1) Despite the definition *personal information* in subsection 2(1), for the purposes of this section, *personal information* means information about an identifiable individual.

#### Collection, use, disclosure, retention and disposal

(2) In order to participate in public affairs by endorsing one or more of its members as candidates and supporting their election, any registered party or eligible party, as well as any person or organization acting on the party's behalf, including the party's candidates, electoral district associations, officers, agents, employees, volunteers and representatives, may, subject to this Act and any other applicable federal Act, collect, use, disclose, retain and dispose of personal information in accordance with the party's privacy policy.

#### Purpose

(3) The purpose of this section is to provide for a national, uniform, exclusive and complete regime applicable to registered parties and eligible parties respecting their collection, use, disclosure, retention and disposal of personal information.

Canadians should be *and are* outraged. Indeed, on April 28, 2023, democracy watchdog Open Media started a Petition<sup>55</sup> against this cynical and hypocritical political maneuver that garnered thousands of Canadian signatures.

Notably, in his Remarks before the Standing Senate Committee on Legal and Constitutional Affairs (LCJC) on May 3, 2023, Privacy Commissioner of Canada Philippe Dufresne made it

---

<sup>55</sup> Specifically, the Petition states "We call on the federal government to remove Division 39, the amendment to *Canada's Elections Act*, from Bill C-47, and add political parties to the definition of organizations in Bill C-27's *Consumer Privacy Protection Act* so that they are explicitly covered by Canada's privacy laws." !

clear that *meaningful* privacy obligations should apply to the FPPs and that the proposal in C-47 was anything but. Specifically, Commissioner Dufresne said:

The proposed amendments to the *Canada Elections Act* in Bill C-47 do not establish minimum privacy requirements for political parties to follow in their handling of personal information or provide for independent oversight of their privacy practices. Rather, the proposed changes would allow political parties and their affiliates to collect, use, retain, disclose, and dispose of personal information in accordance with the party's own privacy policy – which they develop and revise at their own discretion.

Given the importance of privacy and the sensitive nature of the information being collected, Canadians need and deserve a privacy regime for political parties that goes further than self-regulation and that provides meaningful standards and independent oversight to protect and promote electors' fundamental right to privacy.

Political parties should be subject to specific privacy rules that are substantially similar to the requirements that are set out for the public and private sectors in the *Privacy Act* and PIPEDA, while at the same time being adapted to the unique role played by political parties in the democratic process. In other words, privacy requirements that are grounded in legislation, that conform with internationally recognized privacy principles, and that include recourse to an independent third party with authority to verify and enforce compliance and provide remedies in case of a breach. (emphasis added)

Similarly, in his Remarks to the LCJC also on May 3<sup>rd</sup>, Canada's Chief Electoral Officer Stéphane Perrault voiced the following concerns:

Bill C-76 amended the *Canada Elections Act* in 2018 to require parties to publish their own privacy policy, which must include statements indicating the type of information collected and how it is protected and used, under what circumstances information may be sold, how the party collects and uses personal information created from online activity and the name and contact information of a person to whom privacy concerns may be addressed.

While these requirements increase transparency about the handling of personal information by political parties, there are no minimum standards in the Act that parties must follow. Nor is there any oversight mechanism to monitor whether parties abide by the contents of their policies, or any sanctions in case of non-compliance.

In my 2022 recommendations report following the 43rd and 44th general elections, I recommended that the privacy principles enumerated in Schedule 1 of the *Personal Information and Protection of Electronic Documents Act* should apply to registered and eligible parties, with oversight by the Office of the Privacy Commissioner of Canada.

In the absence of full application of these principles, I recommended certain minimal requirements, namely:

- that Canadians have the right to opt out of receiving communications—or certain types of communications—from political parties;
- that they have the ability to request access to, and correct, inaccurate personal information held by political parties; and finally
- that political parties be required to indicate in their policies how electors' personal information may be shared (in addition to how it is collected, used and sold).

Mr. Chair, I believe that better safeguarding electors' personal information will help maintain Canadians' trust in Canada's political parties, and by extension, the electoral process.

That said I want to be clear. I do not believe that such an important reform of the *Canada Elections Act* should take place in the context of a Budget bill, but rather it should be done through a separate bill. (emphasis added)

The Government's amendment to the *Canada Elections Act* in Bill C-47 has nothing to do with “privacy protection”. It is an unconstitutional power grab meant to give the FPPs unregulated reign over Canadians’ personal information. Why are the FPPs tooth-and-nail resistant to abiding by the same privacy rules as the rest of Canadians? What are the FPPs hiding?

*You must do as we say, not as we do. We make the rules. You must obey, but we choose not to.* This sums up precisely the FPPs’ attitude to Canadians’ privacy and personal information.

Such hypocrisy. Canadians across the public and private sector must comply with exacting privacy laws. But the FPPs - whose members make those laws - are exempt. How is this possibly fair or just?

It is shocking that the FPPs are unregulated by any privacy law. Like Google, Facebook and countless smaller organizations in Canada, the FPPs capture, hold and exploit large quantities of sensitive personal and profiling information about Canadians: political views, campaign contributions, voting history, religious affiliation, family status, income range and more. Strong laws govern how Canadian organizations must account for this sensitive information. Except the FPPs. They are unaccountable.

#### *The Budget Proposal, Privacy and the Canada Elections Act*

No one was fooled by the nonchalance of the final phrase of the federal government's March 28, 2023 non-budgetary proposal in the 2023 Budget for “...a uniform federal approach in respect of federal political parties’ collection, use, and disclosure of personal information in a manner that [purportedly] overrides overlapping provincial legislation”. Those words mask a jurisdictional grab by the FPPs, through their elected members, to avoid accountability, purportedly override provincial privacy laws, and retain their unrestrained and self-bestowed privileges over Canadians’ personal information.

The *Canada Elections Act* is not a privacy statute. It is about elections. It cannot be twisted into a robust framework governing the FPPs' collection, use or disclosure of Canadians' personal information. That’s the job of privacy legislation. Asking Elections Canada to govern privacy (which it has neither the expertise nor interest to do) is like asking hospitals to process tax returns.

Canadians must be afforded robust privacy protections. The FPPs must be subject to comprehensive privacy regulations and effective oversight and enforcement. The Centre for Digital Rights has been and is advocating for such measures in this Report on Bill C-27. They are in everyone’s’ interests.



When the FPPs suffer a serious data breach (for which they currently have no obligation to report to any public authority or affected individuals) and international headlines ensue, Canadians' awareness will focus on just out how much profiling and personal information the FPPs have collected, ungoverned by a robust personal information framework. Canadians' trust in the FPPs will be shaken. Goodwill the FPPs have established will be compromised.

*“Overrides ... Provincial Legislation”: A Constitutional Grab*

The government's now-in-force *Canada Elections Act* amendment tramples on the provinces' established constitutional powers. The short word budget fragment did not conceal its intention to purportedly "[override] overlapping provincial legislation".

The government's maneuver – a law purporting to exempt the FPPs from the same privacy legislation they make all other Canadians obey – is not only hypocritical, but also a violation of Canada's Constitution and Canadians' democratic rights under the *Canadian Charter of Rights and Freedoms*.

Section 92 of the *Constitution Act, 1867* grants the provinces full powers over privacy, under the headings of "property and civil rights"<sup>56</sup> and "matters of a merely local or private nature".<sup>57</sup> Using these powers, British Columbia, Alberta, and Quebec have had their own privacy laws for decades.<sup>58</sup>

The purportedly meant-to-be-exclusive *Canada Elections Act* amendments, however framed, are an unwelcome and unconstitutional intrusion on provincial laws. For example, the privacy protections that Quebecers enjoy would be denied to them by and for the FPPs. Private personal information would not be private in the hands of the FPPs if the Québec law was deemed to be "overlapping provincial legislation".

The *Canada Elections Act* regulates one thing: elections. Provincial privacy laws also regulate one thing: privacy, i.e., the collection, use and disclosure of personal information. The two mandates are distinct. Carrying out one does not, should not, and constitutionally must not inhibit the other's capacity to exercise its purpose. The essential character of the proposed *Canada Elections Act* amendments – their “pith and substance” in constitutional parlance – (looking to both their purpose and effect)<sup>59</sup> would not be to run federal elections. It would be to regulate the privacy and personal information of electors. Clearly, this pith and substance places the proposed amendments within the provincial heads of power under section 92 of the *Constitution Act, 1867* mentioned above, i.e., property and civil rights, and matters of a merely local or private nature.

---

<sup>56</sup> *Constitution Act, 1867*, 30 & 31, Victoria, c. 3 (UK), s 92(13).

<sup>57</sup> *Ibid*, s 92(16).

<sup>58</sup> *Personal Information Protection Act*, SBC c 63; *Personal Information Protection Act*, SA 2003, c. P-65; *Act Respecting the Protection of Personal Information in the Private Sector*, P-39.1 (Qué.).

<sup>59</sup> *Chatterjee v. Ontario (Attorney General)*, 2009 SCC 19 at para 17; *Reference re Genetic Non-Discrimination Act*, 2020 SCC 17 at para 28; *Reference re Greenhouse Gas Pollution Pricing Act*, 2021 SCC 11 at paras 51 to 56.

Not even the current federal privacy law, the *Personal Information Protection and Electronic Documents Act* (**PIPEDA**) or its proposed replacement, the *Consumer Privacy Protection Act*, goes so far as to purportedly oust provincial privacy legislation. On the contrary, they both explicitly recognize provincial powers by exempting organizations if a province has enacted substantially similar privacy legislation.

Canadian constitutional law promotes cooperative federalism. By usurping the function of provincial privacy statutes, the *Canada Elections Act* amendments violate the principle of cooperative federalism and offend the presumption that Parliament intends its laws to co-exist with provincial laws.<sup>60</sup> This is not co-existence. It is unconstitutional intrusion.

### *Privacy Laws, “Organizations”, and the FPPs*

Privacy law obligations apply to organizations, so a key factor under all privacy laws is whether the FPPs are “organizations”. Current provincial and federal legislation treat political parties differently.

The federal government exercises limited privacy jurisdiction through its trade and commerce powers under section 91(2) of the *Constitution Act, 1867*. It exercises this jurisdiction through PIPEDA.

PIPEDA defines “organization” as an association, partnership, a person, and a trade union.<sup>61</sup> The Office of the Privacy Commissioner of Canada (**OPC**), which administers PIPEDA, has said that it does not consider PIPEDA to apply to FPPs when their activities are not commercial.

However, the OPC has repeatedly called for FPPs to be subject to legislation based on “internationally recognized privacy principles and provide for an independent third party authority to verify compliance”.<sup>62</sup>

At the same time, the federal *Canada Elections Act* defines an FPP as “an organization one of whose fundamental purposes is to participate in public affairs by endorsing one or more of its members as candidates and supporting their election.”<sup>63</sup>

British Columbia’s *Personal Information Protection Act* (**BC PIPA**) defines “organization” as a person, unincorporated association, a trade union, a trust, and not-for-profit.<sup>64</sup> BC PIPA has been interpreted to apply to both federal and provincial political parties.<sup>65</sup>

---

<sup>60</sup> *Rogers Communications Inc. v. Chateauguay (City)*, 2016 SCC 23 at para 38; *Quebec (Attorney General) v. Canada (Attorney General)*, 2015 SCC 14 at para 17.

<sup>61</sup> PIPEDA, section 2.

<sup>62</sup> [https://www.priv.gc.ca/en/opc-news/news-and-announcements/2021/an\\_210513/](https://www.priv.gc.ca/en/opc-news/news-and-announcements/2021/an_210513/) and [https://www.priv.gc.ca/en/opc-actions-and-decisions/advice-to-parliament/2023/parl\\_20230503/](https://www.priv.gc.ca/en/opc-actions-and-decisions/advice-to-parliament/2023/parl_20230503/)

<sup>63</sup> *Elections Act*, section 2 <https://laws-lois.justice.gc.ca/eng/acts/e-2.01/>

<sup>64</sup> BC PIPA, section 1.

<sup>65</sup> *Conservative Party of Canada (Re)*, 2022 BCIPC 13.

Alberta's *Personal Information Protection Act* (**AB PIPA**) defines “organization” as a corporation, unincorporated association, trade union, partnership, or individual acting in a commercial capacity, but specifically excludes registered political parties.<sup>66</sup>

Quebec’s election legislation was amended to make political parties subject to limited parts of its private sector privacy law, an *Act respecting the protection of personal information in the private sector*. Quebec's election law amendments make clear that political parties cannot collect or use personal information without consent, and that a political party may only collect and use electors’ personal information necessary for election or political financing purposes or for the purposes of a political activity.

The FPPs' activities in Quebec are generally subject to Quebec's *Charter of Human Rights and Freedoms*<sup>67</sup> (**Quebec Charter**) and the *Civil Code of Quebec*<sup>68</sup> (**Civil Code**). Specifically, Article 5 of the *Quebec Charter* states that every person has a right to the respect of their privacy, subject to limitations by law. The *Civil Code* recognizes that every person has a right to the respect of privacy (Article 35), provides limits on the collection, use and disclosure personal information (Article 37), and guarantees that every person has the right to access and correct their personal information (Articles 38-40).

This co-existence of differing treatments of political parties points a cooperative, privacy-respectful way ahead for the FPPs in place of the now in force *Canada Elections Act* amendments.

In addition to unconstitutionally intruding into provincial legislative jurisdiction over privacy rights in the province, the amendments to the *Canada Elections Act* unjustifiably infringe section 3 of the *Charter* – specifically the "right to vote" which the Supreme Court of Canada has interpreted broadly to mean Canadian's meaningful and informed participation in the electoral process.

### *A Cooperative Approach*

Having to comply with both federal and provincial laws is nothing new for Canadian organizations, certainly in the privacy space. Organizations that operate across Canada find themselves having to comply with PIPEDA, BC PIPA, AB PIPA, and Quebec's private sector privacy law, depending on the circumstances.

Similarly, federal and provincial privacy commissioners have demonstrated that they can work together. They have conducted joint investigations into organizations operating within and across borders, including TikTok, Clearview AI, Tim Hortons, Facebook, Cadillac Fairview, and AggregateIQ Data Services.

---

<sup>66</sup> AB PIPA, section 1.

<sup>67</sup> CQLR c. C-12.

<sup>68</sup> CQLR c. C-1991.

A similar cooperative approach should and must be adopted regarding the FPPs. The *Canada Elections Act* amendments read as an arrogant attempt to brush aside provincial constitutional powers and let the FPPs out of complying with laws all other Canadians must obey. With respect to the appropriate federal law, there is no public policy rationale whatsoever that the privacy protection practices of the FPPs should not be regulated under Bill C-27 with oversight and enforcement by the OPC.

The FPPs, through their members in Parliament, cannot be allowed to oust the provinces' constitutional privacy powers in such a brazenly self-dealing manner. It would be just as wrong for them to try and do so as it would for the provinces to attempt a takeover of Canada Post.

Any FPP exemption from provincial privacy laws is unlikely to survive the court challenges that are sure to follow. More importantly, it will erode public confidence in the FPPs at a time when such confidence is in sore need of reinforcement.

**Appendix H**  
**Summary of new points in CDR's Report on C-27 dated October 2, 2023 updating CDR's**  
**C-27 Statement on C-27 dated October 28, 2022**

This Report expands on and updates CDR's October 28, 2022 Statement on Bill C-27 as follows:

1. **Indigenous data sovereignty:** adding a new recommendation 2.3 (under "framing the purposes of Bill C-27 properly") that the federal government consult with Indigenous Peoples and recognize Indigenous Sovereignty over their data;
2. **Federal political parties (FPPs):** adding in recommendation 3.1 ("expressly extend the federal private sector privacy law to cover Canada's federal political parties") that (a) the Australian Government, in its Attorney-General's Department's Privacy Act Review Report 2022 , published on February 16, 2023, has recommended that registered political parties in Australia be covered by the same private sector privacy law that governs all private sector organizations and (b) the federal government's recent amendments to the *Canada Elections Act* purportedly to provide for a uniform federal approach in respect of the FPPs' collection, use and disclosure of Canadians' personal information in a manner that overrides overlapping provincial legislation is not only hypocritical, it would be a violation of Canada's Constitution and *Charter*;
3. **Consent on digital media:** adding a new recommendation 5.4 (under "fix the consent" provisions) that any online collection, use or disclosure of an individual's personal information for purposes beyond what is necessary to provide a product or service requires an express, opt-in, revocable consent from the individual that is separate from the individual's agreement to the terms of use of the service such that the privacy consent is not a condition of the service. This addition is intended to capture the evolving standard for online data collection articulated in the recent decisions of the European Data Protection Board (on December 5, 2022) and the Irish Data Commission (on December 31, 2022) in the *Meta Ireland* cases against Facebook and Instagram and by the Office of the Privacy Commissioner of Canada in its January 26, 2023 *Home Depot* Report of Findings;
4. **Rewriting CPPA's consent and legitimate interests provisions:** including in new recommendation 5.5, a proposed re-write of sections 15 and 18(3) of the CPPA to address CDR's concerns in recommendations 5.1 to 5.4;
5. **Non-identifiable information:** adding to recommendation 7.7 (under "adjust the CPPA's proposed regime for non-identifiable information") a reference to the December 7, 2022 Submission on Bill C-27 of the Canadian Anonymization Network (CANON);
6. **Privacy by design and control by design:** adding to recommendation 11.1 (under "for further study" and with respect to the concept of "control by design" and its advantages over "privacy by design") a reference to ISO's January 2023 "privacy by design" Standard (ISO 31700-1) and Technical Report (ISO/TR 31700-02);

7. **A complaint funding mechanism:** adding as a new recommendation 11.4 (under "for further study") that the federal government, inspired by options currently under consideration in Europe and models already in place in Canada, consider establishing a complaint funding mechanism (which could draw funds from the private sector, public sector, or both) to help finance legal proceedings brought by individual or group complainants and/or public interest organizations seeking remedies against organizations for alleged contraventions of the CPPA;
8. **Robust privacy regulation encourages trust and advances responsible innovation:** adding to Appendix D ("busting the myth that stricter privacy regulation stifles innovation") further studies that look at the economic impact of the GDPR and the "Brussels Effect", namely how European regulation can elevate and have elevated global standards;
9. **Additions to Bibliography:** adding several publications to Appendix I (the "annotated bibliography") including op-eds recently published by Professors Bennett and Clement and new articles including two on AIDA by Professor Scassa;
10. **Critique of Canadian Marketing Association's position:** adding as new Appendix E CDR's critique of the CMA's Privacy Reports of February and October 2022.<sup>69</sup> This critique was prepared at the request of the CMA following Jim Balsillie's meeting on January 9, 2023 with the CMA's Privacy and Data Protection Committee;
11. **Critique of ISED's Companion Document for AIDA and consultation regarding a voluntary industry code of practice for generative AI:** adding as new Appendix F, CDR's critique of ISED's companion document for AIDA released on March 13, 2023 nine months after tabling AIDA in the House of Commons on June 16, 2022. See also Professor Clement's critique of ISED's consultation in August and September of a voluntary code for generative AI systems; and
12. **Critique of the federal government's amendments to the *Canada Elections Act* to provide for a so-called "uniform approach" to privacy laws for the FPPs:** adding as new Appendix G, CDR's Constitutional and *Charter* critique of the federal government's amendment of the *Canada Elections Act* announced on March 28, 2023 and that received Royal Assent on June 22, 2023.

---

<sup>69</sup> In addition to the serious flaws of the CMA's Privacy Reports described in CDR's March 7, 2023 letter to the CMA, following a careful review of the statements made in the CMA's February 2022 Privacy Report and the sources for those statements cited in the footnotes, CDR is of the view that this particular CMA report (alleging various pitfalls of the GDPR) is out-of-date, out-of-context, and out of touch. The report relies on old news and leaves out new facts. It ignores crucial research and paints a misleading picture that favours industry and neglects consumers. It is not properly and independently researched and should not be used to form the basis of public policy.

## Appendix I Annotated bibliography

*This annotated bibliography provides links to some of the latest research, analysis and additional information on many of the subjects discussed in this Report. It aims to assist policy makers, stakeholders, academics, professionals and other interested parties with additional materials on privacy modernization related topics.*

1. Addario, Frank and Samara Selter, Addario Law Group LLP, "Opinion Prepared for the Office of the Privacy Commissioner of Canada: The Constitutional Validity of Bill C-11, the Digital Charter Implementation Act", (*Office of the Privacy Commissioner of Canada*, March 31, 2022), online: [https://www.priv.gc.ca/en/opc-news/news-and-announcements/2022/op-c11\\_addario/](https://www.priv.gc.ca/en/opc-news/news-and-announcements/2022/op-c11_addario/)

Privacy Commissioner of Canada retained Addario Law Group LLP to provide a legal opinion regarding the constitutionality of Bill C-11 – the *Digital Charter Implementation Act, 2020*. The legal opinion found that, given the development in division of powers jurisprudence over the last five years and the prevalence of the digital economy, a court would find Bill C-11 constitutional and a valid exercise of the Federal Trade and Commerce Power. **The opinion also looked at the Privacy Commissioner's suggested proposed amendments to Bill C-11, namely whether the addition of a preamble (that explicitly included the recognition of privacy as a basic human right) and other amendments changed the pith and substance of the Bill away from its economic focus. The opinion found that none of the amendments proposed by the Privacy Commissioner changed the pith and substance of the Bill and that in fact, some of the amendments will add to the constitutional validity of the Bill by clarifying the centrality of the national economy to the Bill and its promotion through stringent privacy protection.**

2. Anderljung, Markus and Joslyn Barnhart, Jade Leung, Anton Korinek, Cullen O'Keefe, Jess Whittlestone, Shahar Avin, Miles Brundage, Justin Bullock, Duncan Cass-Beggs, Ben Chang, Tatum Collins, Tim Fist, Gillian Hadfield, Alan Hayes, Lewis Ho, Sara Hooker, Eric Horvitz, Noam Kolt, Jonas Schuett, Yonadav Shavit, Divya Siddarth, Robert Trager, Kevin Wolf, "Frontier AI Regulation: Managing Emerging Risks to Public Safety", (Cornell University, July 2023), online: <https://arxiv.org/abs/2307.03718>  
The paper looks at balancing public safety risks and innovation in the development and advancement of AI. It focusses on "frontier AI" models – models which could possess dangerous capabilities sufficient to pose a severe risk to public safety. There are three factors that suggest frontier AI development needs targeted regulation: (1) models may possess unexpected and difficult to detect dangerous capabilities; (2) models deployed for broad use can be difficult to reliably control and to prevent from being used to cause harm; and (3) models may proliferate rapidly, enabling circumvention of safeguards. Self regulation is unlikely to provide sufficient protection against the risks from frontier AI models and government intervention will be needed. Options for intervention include mechanisms to create and update safety standards, mechanisms to give regulators

visibility, and mechanisms to ensure compliance with safety standards. Some safety standards or guardrails include conducting thorough risk assessments informed by evaluations of dangerous capabilities and controllability, engaging external experts to apply independent scrutiny to models, following standardized protocols for how frontier AI models can be deployed based on their assessed risk, and monitoring and responding to new information on model capabilities.

3. Ansari, Mehwish & Vidushi Marda, "AI Act — leaving oversight to the techies will not protect rights", (EUObserver, 5 May 2023), online: <https://euobserver.com/opinion/156992>

The authors state that the two key European committees identified in the EU AI Act to develop standards, technical frameworks, requirements, and specification for high-risk AI technologies may not be the best positioned to ensure people's fundamental rights are truly protected. The authors point out that these Committees, the European Committee for Standardisation (CEN) and the European Committee for Electrotechnical Standardisation (CENELEC), are almost exclusively composed of engineers or technologists with little to no representation from human rights experts or civil society organizations, raising concerns that they will have the de facto power to determine how the AI Act is implemented, yet without the means to ensure people's fundamental rights are met. The authors discuss that not enough attention is being paid to how "high risk" applications of AI systems will be implemented in practice, and that it is impossible to completely separate design choice from real world impacts on individual rights. The authors state that outsourcing these considerations to technical bodies is not the answer to regulating AI in a way that respects human rights and suggest that a better way forward includes establishing fundamental rights impact assessment frameworks as a requirement for all high-risk AI systems, before such systems can be placed on the market.

4. Balkin, Jack M., "The Fiduciary Model of Privacy", (Harvard Law Review, November 2020), online: [https://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=3700087](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3700087)

This article summarizes and restates the theory of information fiduciaries and the fiduciary model of privacy. It argues that, **because of the vulnerability and dependence created by information capitalism, the law should regard digital companies that collect and use end user data as information fiduciaries**. Fiduciary duties "run with the data": digital companies must ensure that anyone who shares or uses the data is equally trustworthy and is legally bound by the same legal requirements of confidentiality, care, and loyalty as they are. The articles states that once implemented, **the fiduciary model will give digital businesses legal incentives to act in the interests of their end-users**, interests which they often claim to respect but actually do not. The article concludes with a proposal for imposing fiduciary obligations on businesses.

5. Balsillie, Jim, "Privacy is central to human well-being, democracy, and a vibrant economy. So why won't the Trudeau government take it seriously? The Globe and



Mail, October 22, 2022, online: <https://www.theglobeandmail.com/opinion/article-digital-privacy-technology-canada/> [Note: Behind paywall]

The author shines a light on the main flaws of Bill C-27 and critiques its many failures for both Canadians and Canadian businesses including that, by the federal government prioritizing business interests, the proposed legislation (1) normalizes and expands surveillance capitalism, (2) fails to make privacy a fundamental human right, (3) continues to rely on the widely-discredited primacy-of-consent model, (4) creates overly broad exceptions to consent for businesses (including the ill-conceived "legitimate interests" exception) that neither protect Canadians' privacy nor spurs innovation, (5) does next to nothing to protect minors and ignores progressive laws recently passed in the UK and in California that pay special attention to protecting the privacy rights of children, and (6) fails to provide, in the proposed Artificial Intelligence and Data Act (AIDA), even the shell of a framework for responsible artificial intelligence/automated decision systems regulation and oversight.

6. Bannerman, Sara, Julia Kalinina, Elizabeth Dubois and Nicole Goodman, "Privacy and Canadian Political Parties: The Effects of the Data-Driven Campaign on Elector Engagement.", (*Canadian Journal of Political Science* 1-24, October 2022), online: <https://doi.org/10.1017/S000842392200066X>,

The authors report the results of a survey examining Canadian's attitudes about political parties' collection of personal information and its potential impact on elector engagement. **Among other takeaways, the authors find that the application of privacy law to political parties is warranted. The survey results corroborate views from past surveys conducted by the Centre for Digital Rights and the Office of the Privacy Commissioner of Canada in finding that over 85% of Canadians believe that political parties should be subject to privacy law.**

7. Bednar, Vass, "Debating the Right Balance(s) for Privacy Law in Canada", (Public Policy Forum, January 2022), online: <https://ppforum.ca/publications/debating-the-right-balances-for-privacy-law-in-canada/>

This report is a summary of roundtable debates and discussions that took place between academics, lawyers, representatives from the private sector and members of civil society under Chatham House rules. Hosted by the Public Policy Forum, the discussions centered on key questions concerning privacy modernization and how Canada compares to other regimes around the world. Debate from the roundtables demonstrates that **some participants are optimistic that a human rights approach to privacy can co-exist with data-driven private sector innovation. As well, there was skepticism regarding the utility of a new privacy Tribunal that could be separate from that of the Privacy Commissioner. The report also notes that the exemption of political parties from requirements placed on the private sector represents a misalignment.** Treatment should be consistent between non-profit and charitable organizations and political

parties. Overall, stakeholders believe that a coherent privacy framework that better protects Canadians and empowers responsible innovation is achievable through harmonizing approaches introduced by Canadian provinces and learning from path-breaking international peers.

8. Bennett, Colin, "Canada Introduces Three New Privacy Bills to Modernise Privacy Law", *Privacy Laws and Business*, August 2022), online: <https://www.privacylaws.com/reports-gateway/reports/> [Note: *Behind paywall.*]

The article examines the introduction of recently tabled privacy bills in Canada, namely Bill C-27 and its predecessor, former Bill C-11. The article explains how Bill C-11 was subject to criticism from all sides of the political spectrum, and how Bill C-27 has had significant amendments, however **a large portion of the former Bill C-11 has been retained in Bill C-27**, likely leaving privacy advocates disappointed. The article explains that there is no specific mention that privacy is a fundamental human right in Bill C-27, that the consent-based privacy framework for processing personal data remains, and highlights the changes to the definitions of de-identified and anonymized information. The article also describes the new AI Act, stating that, it has the appearance of being a bit of an "empty shell" where much is left up to future regulation.

9. Bennett, Colin J., "Privacy czar's Home Depot investigation exposes weaknesses in Ottawa's new privacy bill," *The Hill Times*, February 23, 2023, online, <https://www.hilltimes.com/story/2023/02/23/privacy-czars-home-depot-investigation-exposes-weaknesses-in-ottawas-new-privacy-bill/379346/>

The author examines the Office of the Privacy Commissioner of Canada's (OPC) Report of Findings into Home Depot to show the limitations of the implied consent provisions in Bill C-27. The author argues the implied consent provisions in Bill C-27 should be eliminated since they create confusion for both consumers and businesses. In the Home Depot case, the OPC found that proper consent was not obtained for the disclosure of information to Meta (Facebook) for its "offline conversations" service. The author shows how a continued reliance on implied consent raises serious questions about the implied consent provisions in the *Consumer Privacy Protection Act* (CPPA), contrasting its consent provisions with the protections afforded under Europe's *General Data Protection Regulation* (GDPR), where consent means express consent. The author states that Bill C-27 allows businesses to have both the options of legitimate interests and implied consent, which needs to be fixed in upcoming parliamentary consideration of Bill C-27.

10. Bennett, Colin J., ""Privacy Is Like Yoga"- and Other Myths", (*Centre for International Governance Innovation*, February 8, 2023), online: <https://www.cigionline.org/articles/privacy-is-like-yoga-and-other-myths/>

The author calls out several misheld beliefs (touted often by industry resisting change to the *status quo*) about data privacy laws. First, he questions the idea that privacy law must always balance individual's rights with organization's needs. He notes that continued

rhetoric regarding balance has permitted business models and practices once considered unacceptable to be normalized over time. Second, he disagrees with the notion that privacy law must always be technologically neutral. He states that some technologies are inherently intrusive and repressive and that they should not be afforded neutral treatment. Third, he challenges assumptions about the GDPR including that it is overly rigid and prescriptive, is not based on flexible principles, is based solely on EU concepts, and is a one-size-fits all regime. He comments that the GDPR is principles-based and that it represents a product of compromise fought over for many years between different interests. Lastly, he rebuts the assumption that Canada needs a made-in Canada privacy law distinct from the GDPR. He states that the digital economy does not change its character when it hits Canada's border and highlights the fact that numerous large international companies (Apple, Microsoft etc.) and over 140 countries have been influenced by the GDPR in improving their operational standards and passing data privacy laws, respectively.

11. Bennett, Colin, "One set of privacy rights for Europeans, a lesser one for Canadians? Why the Canadian consumer privacy protection act and the EU's general data protection regulation should be in alignment", (May 20, 2021), online: <https://www.colinbennett.ca/canadian-privacy/one-set-of-privacy-rights-for-europeans-a-lesser-one-for-canadians-why-the-canadian-consumer-privacy-protection-act-and-the-eus-general-data-protection-regulation-should-be-in-alignment/>

In this blog post, the author discusses how some large or multinational companies operating in Canada are seeking GDPR compliance, and contrasts how Canadians could have a lesser standard of privacy protection than Europeans even by the same company, where a company has put in GDPR compliance for European data, but not for Canadian data. The author states that privacy modernization in Canada should be in alignment with the GDPR to strengthen the rights of Canadians so that Canadians do not have a lesser standard of privacy protection.

12. Bradford, Anu, "The Brussels Effect: How the European Union Rules the World" (2020). Columbia Law School *Faculty Books*. 232, online: <https://scholarship.law.columbia.edu/books/232>

In this book, the author analyzes the "Brussels Effect", which refers to the influence of regulation in the European Union outside of Europe, how multinational corporations elevate their regulatory standards in response to compliance with EU legislation, and how EU standards become global standards.

13. Bremmer, Ian and Mustafa Suleyman, "The AI Power Paradox", (Foreign Affairs, 2023), online: <https://www.foreignaffairs.com/world/artificial-intelligence-power-paradox>

The authors argue for a 'technoprudentialist' approach to AI regulation, meaning that the overarching goal of any global AI regulatory architecture should be to identify and mitigate risks to global stability without choking off AI innovation and the opportunities that flow from it. The authors state that AI cannot be governed like any previous

technology and suggest a new governance framework aligned with the uniqueness of the technology. The "AI power paradox" relates to AI's hyper revolutionary nature which makes solving its challenges, including around policy and power dynamics, progressively harder. The authors state there is little use in regulating AI in some countries if it remains unregulated in others and suggest that AI governance have no gaps, noting the challenges of today's geopolitics. 'Technoprudentialism' includes a mandate similar to the macroprudential role played by global financial institutions – their objective is to identify and mitigate risks without jeopardizing economic growth. The authors argue that AI governance should be precautionary, agile, and inclusive, inviting the participation of all actors needed to regulate the practice. The authors also state that there should be a minimum of three AI governance regimes, one focussing on fact-finding to objectively advise governments and international bodies (for example, akin to the Intergovernmental Panel on Climate Change), another to manage tensions between the major AI powers and prevent the proliferation of dangerous advanced AI systems, and another that can react when dangerous disruptions occur, akin to the Financial Stability Board, who works to prevent global instability by assessing systemic vulnerabilities and coordinating necessary actions to address them among national and international authorities.

14. Borrows, John and Lisa Austin, "The Digital Charter Implementation Act ignores Indigenous Data Sovereignty", (commentary, University of Toronto, Schwartz Reisman Institute for Technology and Society, December 6, 2022), online: <https://srinstitute.utoronto.ca/news/digital-charter-implementation-act-ignores-indigenous-data-sovereignty>

The authors state that Bill C-27 has left out Indigenous voices, noting that what has been absent is serious consultation with Indigenous communities and any attention at all to whether Bill C-27 is consistent with the federal government's obligation to implement the United Nations Declaration on the Rights of Indigenous Peoples (UNDRIP). The authors note that a number of provisions in Bill C-27 could better align with Indigenous laws and values, and states that the landscape of Canadian data laws ignores the principles of Indigenous self-determination and self-government. The authors point out how Bill C-27 permits the disclosure of de-identified information without knowledge or consent for "socially beneficial purposes" however, there is no requirement that where this information pertains to Indigenous communities that there be authorization from those communities. Several provisions of Bill C-27 should be re-examined through an Indigenous Data Sovereignty lens.

15. Chen, Chinchih, Carl Benedikt Frey, and Giorgio President, "Privacy Regulation and Firm Performance: Estimating the GDPR Effect Globally", (Oxford Martin School, University of Oxford, January 6, 2022), online: <https://www.oxfordmartin.ox.ac.uk/downloads/Privacy-Regulation-and-Firm-Performance-Giorgio-WP-Upload-2022-1.pdf>

Through a study of companies across 61 countries and 34 industries, the authors examine the effect of the GDPR's introduction on firm performance. They conclude that the

GDPR's enhanced data protection measures and associated compliance costs have caused an 8% decline in profitability for firms targeting European consumers, with an exacerbated impact on smaller companies. That said, the authors highlight three reasons to interpret their findings with caution: (1) given the GDPR's recency, firms likely incurred temporary adjustment costs through the form of investments in new GDPR-compliant technologies, which may taper off in the future, (2) if the GDPR gradually becomes a global standard, companies targeting EU consumers will become less disadvantaged over time, and (3) negative impacts on profitability do not account for aggregate welfare effects, including benefits to citizens concerned with data protection. The authors state that this latter point represents an important line of future inquiry. Furthermore, the authors state "Though there is widespread concern that the GDPR has reduced digital innovation in Europe, it is equally plausible that it has accelerated innovation by inducing companies to develop new GDPR-compliant technologies".

16. Clement, Andrew, "One way we could fund our privacy watchdog", *The Globe and Mail* (Ontario Edition), March 3, 2023, online: <https://www.theglobeandmail.com/business/commentary/article-privacy-commissioner-funding/>

In this op-ed published in *The Globe and Mail*, Professor Andrew Clement looks at a "polluter pays" funding model for privacy regulators. The author contrasts the enormous profits that big tech companies acquire through their targeted advertising services with the underfunding of the Office of the Privacy Commissioner of Canada and suggests regulators be funded in part from those who monetize personal information for commercial gain.

17. Clement, Andrew "The Artificial Intelligence and Data Act needs a reset", *The Hill Times*, November 23, 2022, online, <https://www.hilltimes.com/story/2022/11/23/the-ai-and-data-act-needs-a-reset/356482/>

The author argues the *Artificial Intelligence and Data Act* (AIDA) is flawed legislation and should be sent back to the drawing board. The author points to examples of recent uses of AI in social media, facial recognition technology, mass data collection, and points to the growing public concern about the misuse of complex algorithmic systems. The author states that the AIDA was written too hastily, noting that it skipped the normal public consultation process and was introduced along side the *Digital Charter Implementation Act*, whereas it should have been separated from the rest of Bill C-27 for substantial reworking. The author suggests that redrafting the AIDA should include genuine public consultation, looking to the European Union's *Artificial Intelligence Act*, engaging community advocates, researchers, lawyers, and representatives of at-risk populations. The author states that the AIDA should have independent regulatory oversight, that the scope of harms should include collective and not just individual harms,

and that the scope of relevant algorithmic practices should be widened to focus on function and not a narrow set of specific techniques.

18. Cropper, Lorna, "Data Protection and Digital Information (No. 2) Bill, Take Two" (Fieldfisher, April 14, 2023), online: <https://www.fieldfisher.com/en/services/privacy-security-and-information/privacy-security-and-information-law-blog/data-protection-and-digital-information-no-2-bill>

The author reviews the impact of the proposed changes of the U.K.'s Data Protection and Digital Information (No. 2) Bill (the "**Bill**"). The author concludes their review by finding that the impact of the Bill in its current form will arguably bring only a "ripple". The author notes that given the remarkably high data protection standards of the E.U., the U.K. government has limited room to manoeuvre and for this reason, the Bill does not "overhaul the data protection landscape".

19. Consultative Committee of Convention, "Guidelines on the Protection of Individuals with regard to the Processing of Personal Data by and for Political Campaigns", (Council of Europe, November 19, 2021), online: <https://rm.coe.int/guidelines-on-data-protection-and-election-campaigns-en/1680a5ae72>

The Council of Europe (**COE**), specifically the Consultative Committee of Convention 108, has published guidelines on the use and processing of personal information for political campaigns. These guidelines aim to provide practical advice to data protection authorities and political organizations and state that processing for the purpose of political campaigns should comply with the COE's modernized Convention 108.

20. Dubois, Elizabeth, "Federal election 2021: Why we shouldn't always trust 'good' political bots", (September 19, 2021), online: <https://theconversation.com/federal-election-2021-why-we-shouldnt-always-trust-good-political-bots-168137>

This article considers whether **AI bots** (such as **Areto Labs SAMbot** and **Advanced Symbolics' Polly**) and surveying technologies, used and operated by non-partisan players, have received misplaced trust. It notes that these technologies represent "black boxes" and that their inputs and operations are not transparent to users or other interested parties. The author suggests steps to better understand and evaluate AI bots moving forward. First, **unavoidable biases should be explicitly acknowledged so that findings can be situated and interpreted appropriately**. Second, **the training processes that develop the technologies should be made available for public scrutiny**. Third, **expectations should be set regarding transparency and clarity**.

21. First Nations Information Governance Centre, "Exploration of the Impact of Canada's Information Management Regime on First Nations Data Sovereignty", (August 22, 2022), online: <https://fnigc.ca/wp->

content/uploads/2022/09/FNIGC\_Discussion\_Paper\_IM\_Regime\_Data\_Sovereignty\_EN.pdf

This paper discusses the conflicts between the current Canadian information management regime and First Nations data sovereignty. It examines the federal governments' discussion papers on the reform of the Privacy Act and the Access to Information Act and states that to respect First Nations data sovereignty, a system wide review of Canada's information management regime is required. The paper presses for changes to the Privacy Act and associated legislation and identifies areas for reform. The paper states that First Nations data sovereignty is an element of their inherent, Treaty, and constitutional rights to self-determination and self-government and that First Nations data sovereignty means First Nations data is governed by First Nations laws. It incorporates the First Nations principles of OCAP® – ownership, control, access, and possession of data. (OCAP® is a registered trademark of the First Nations Information Governance Centre). The paper highlights the systemic barriers to First Nations data sovereignty, including unilateral decision-making by the Crown, a conflict of values and the imposition of an individualistic regime and forced dependence on the private law of contracts to fill a gap in public law. It also addresses: the over-collection of First Nations data and information, the sale of access to First Nations data by the Crown to third parties, a reliance on flawed consent provisions by the Crown to grant itself authority to use First Nations data, the use of First Nations data in a manner that sustains negative stereotypes; and the creation of roadblocks to First Nations access to their data and information. The paper also offers interconnected, multifaceted suggestions for further exploration that may offer short-term and long-term improvements of the system.

22. First Nations Information Governance Centre, "PIPEDA and First Nations: Application and Reform", (First Nations Information Governance Centre, March 2023), online: [https://fnigc.ca/wp-content/uploads/2023/07/PIPEDA-and-FN-Report\\_PROOF-002.pdf](https://fnigc.ca/wp-content/uploads/2023/07/PIPEDA-and-FN-Report_PROOF-002.pdf)

The paper examines the application of PIPEDA and provincial private sector privacy legislation to First Nations businesses, governments, and organizations. It considers First Nations data sovereignty and the First Nations Principles of OCAP® in its analysis of PIPEDA and personal information privacy. The paper outlines and points to several important decisions and guidance documents pertaining to Band Councils. It examines Bill C-27 and uses an overview of the United Nations Declaration on the Rights of

Indigenous Peoples (UNDRIP) to both critique and roadmap Canadian private sector privacy law reform from the perspective of First Nations data sovereignty.

23. Gunst, Simona and De Ville, Ferdi. "The Brussels Effect: How the GDPR Conquered Silicon Valley", *European Foreign Affairs Review*, Volume 26, Issue 3 (2021) pp. 437 – 458, online: <https://doi.org/10.54648/eerr2021036> (Behind paywall)

The authors examined whether the Brussels Effect causally connects the California Consumer Privacy Act (CCPA) with the GDPR based on three sets of evidence: the privacy policies of Apple, Google, and Facebook, lobbying efforts, and whether the California government used arguments linked to the Brussel Effects while drafting the CCPA. The authors conclude that the Brussels Effect did play a role in the adoption of the CCPA and that the impact of the Brussel Effect varies depending on GDPR provision.

24. Office of the Information & Privacy Commissioner for British Columbia, "Guidance Document, Political Campaign Activity", (August 2022), online: <https://www.oipc.bc.ca/guidance-documents/3700>

This guidance document by the Office of the Information and Privacy Commissioner for British Columbia (OIPC) provides best practices for political organizations and their handling of personal information as part of the campaign process. It is especially important as **BC's *Personal Information Protection Act (PIPA)* applies to the collection, use, and disclosure of "personal information" by political parties in British Columbia.** The document examines how political organizations may collect and use personal information, how organizations should notify individuals regarding collection, what constitutes a reasonable purpose and how organizations can implement robust privacy management programs. It complements the OIPC's *Political Campaign Activity Code of Practice*.

25. Office of the Information & Privacy Commissioner for British Columbia, "Political Campaign Activity Code of Practice", (March 2021), online: <https://www.oipc.bc.ca/guidance-documents/3653>

This Code, written by the OIPC and Elections BC, seeks to establish voluntary ground rules for a level playing field between electoral campaigns and to balance the role of political parties with the protection of individual privacy. It asks political parties to commit to ten fair campaigning practices ranging from obtaining meaningful consent to applying adequate privacy protections through a privacy management program.

26. 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, online: [priv.gc.ca/en/opc-actions-and-decisions/submissions-to-consultations/sub\\_indu\\_c27\\_2304/](https://www.priv.gc.ca/en/opc-actions-and-decisions/submissions-to-consultations/sub_indu_c27_2304/)

In the OPC's submission on Bill C-27 to INDU, the Federal Privacy Commissioner, Philippe Dufresne, referred to Bill C-27 as "a step in the right direction" but stated that the Bill "can and must be further improved". The OPC's submission contains 15 Key Recommendations with suggested amendments for Bill C-27, as well as an appendix, which lists additional ways to further enhance Bill C-27, based on the OPC's previous recommendations on the former Bill C-11. The OPC key recommendation #1 states that privacy be recognized as a fundamental right, in both the preamble and section 5 of the CPPA. The OPC suggests that this enhanced preamble be embedded throughout the PIDPTA and the AIDA in addition to the CPPA. OPC key recommendation 2 is to protect children's privacy and the best interests of the child. The OPC recommends that the preamble to Bill C-27 be amended to include an explicit reference which recognizes that the processing of personal data should respect children's privacy and the best interests of the child. Other OPC key recommendations include: expanding the list of violations qualifying for AMPs (at minimum including the appropriate purposes violations), to provide greater flexibility in the use of voluntary compliance agreements to help resolve matters without the need for more adversarial processes, to create a culture of privacy by requiring organizations to build privacy into the design of products and services and to conduct PIAs for high-risk initiatives, and to provide a right of disposal even when a retention policy is in place.

27. Office of the Privacy Commissioner of Canada, Submission on Bill C-11, the *Digital Charter Implementation Act, 2020*, May 2021, online: [https://www.priv.gc.ca/en/opc-actions-and-decisions/submissions-to-consultations/sub\\_ethi\\_c11\\_2105/](https://www.priv.gc.ca/en/opc-actions-and-decisions/submissions-to-consultations/sub_ethi_c11_2105/)

In this landmark submission, the Privacy Commissioner said that former Bill C-11 represented a step back overall for privacy protection and needed significant changes under three main themes: (1) a better articulation of the weight of privacy rights and commercial interests, (2) specific rights and obligations, and (3) access to quick and effective remedies and the role of the OPC. The submission recommends over 65 detailed amendments to Bill C-11 including that federal private sector privacy law should make privacy a fundamental human right.

*See following related paper*

Scassa, Teresa, "Bill C-11's Treatment of Cross-Border Transfers of Personal Information", (University of Ottawa, May 2021), online: [https://www.priv.gc.ca/en/opc-actions-and-decisions/research/explore-privacy-research/2021/tbdf\\_scassa\\_2105/](https://www.priv.gc.ca/en/opc-actions-and-decisions/research/explore-privacy-research/2021/tbdf_scassa_2105/)

The paper, commissioned by the Office of the Privacy Commissioner of Canada (OPC), sets out key considerations to be addressed in a privacy protection framework that addresses trans-border data flows. The author examines the provisions in Bill C-11, specifically the CPPA, and provides a critical analysis of the extent to which its provisions protect privacy. The author also compares the provisions in the CPPA to the measures afforded under comparable jurisdictions and makes twelve recommendations for how the CPPA in Bill C-11 could be enhanced to better protect privacy in the context of international transfers. Specifically, the author recommends that the CPPA should have a dedicated section to address cross-border data flows. Several of the recommendations also point to how the CPPA could be amended, for example, in order to have clear, unambiguous provisions with regards to the trans-border context. The OPC's submission on Bill C-11 (referenced above), relied heavily on this paper in making its recommendations on trans-border data flows.

28. Office of the Privacy Commissioner of Canada, "2022-23 Survey of Canadians on Privacy-Related Issues", (March, 2023), online: [https://www.priv.gc.ca/en/opc-actions-and-decisions/research/explore-privacy-research/2023/por\\_ca\\_2022-23/](https://www.priv.gc.ca/en/opc-actions-and-decisions/research/explore-privacy-research/2023/por_ca_2022-23/)

The OPC survey notes that concerns about the protection of their privacy remains high among Canadians, with 93% expressing some level of concern. The survey also found that fewer Canadians believe businesses respect their privacy rights, and Canadians are least likely to trust social media companies. Only 1 in 10 Canadians trust social media companies to protect their personal information.

29. Office of the Privacy Commissioner of Canada, "2020-21 Survey of Canadians on Privacy Related Issues", (March, 2021), online: [https://www.priv.gc.ca/en/opc-actions-and-decisions/research/explore-privacy-research/2021/por\\_2020-21\\_ca/](https://www.priv.gc.ca/en/opc-actions-and-decisions/research/explore-privacy-research/2021/por_2020-21_ca/)

This biennial survey commissioned by the Privacy Commissioner of Canada and conducted by Phoenix Strategic Perspectives Inc. seeks to better understand the extent to which Canadians are aware of, understand and perceive privacy-related issues. **The survey notes that Canadians are only marginally more concerned about security than privacy (89% to 87%). Further, it finds that Canadians' concerns about public sector use of personal information (PI) do not outweigh concerns about private sector use of PI.** Canadians feel slightly more informed about how their PI is handled by the public-sector (a 3% difference) and are far more confident that the federal government respects their privacy rights compared to private businesses (an 18% difference).

30. Parson, Christopher & Amanda Cutinha, "Minding Your Business: A Critical Analysis of the Collection of De-identified Mobility Data and Its Use Under the Socially Beneficial and Legitimate Interest Exemptions in Canadian Privacy Law", Citizen Lab, Research

Report #161, (November 22, 2022), online: <https://citizenlab.ca/wp-content/uploads/2022/11/Report161-Minding-Your-Business.pdf>

The authors state that Bill C-27 fails to correct existing deficiencies in PIPEDA and proposes 19 legislative amendments to Bill C-27 that would enhance corporate and government accountability for the collection, use, and disclosure of information about Canadian residents and communities, including for de-identified information. In particular, the authors critically assess the government's practice of collecting mobility information for socially beneficial purposes as well as private organizations' ability to collect and use personal information without first obtaining consent from individuals or providing them with knowledge of the commercial activities. The report consists of 5 Parts: Part 1 provides a background of key privacy issues that were linked to collecting mobility data during the COVID-19 pandemic; Part 2 summarizes and identifies key findings from the ETHI meeting sessions on how the federal government obtained and used mobility data over the course of the COVID-19 pandemic; Part 3 assesses the legality of how mobility data can be and has been obtained and used by the federal government; Part 4 identifies six thematic deficiencies in Canada's commercial privacy legislation: 1. PIPEDA fails to adequately protect the privacy interests at stake with de-identified and aggregated data despite risks that are associated with re-identification, 2. PIPEDA lacks requirements that individuals be informed of how their data is de-identified or used for secondary purposes, 3. PIPEDA does not enable individuals or communities to substantively prevent harmful impacts of data sharing with the government, 4. PIPEDA lacks sufficient checks and balances to ensure that meaningful consent is obtained to collect, use, or disclose de-identified data, 5. PIPEDA does not account for Indigenous data sovereignty nor does it account for Indigenous sovereignty principles in the United Nations Declaration on the Rights of Indigenous Peoples, which has been adopted by Canada, and 6. PIPEDA generally lacks sufficient enforcement mechanisms. Part 5 of the report analyzes relevant sections of the CPPA and argues that it does not address deficiencies in PIPEDA and, instead possesses a series of problems.

31. Scassa, Teresa, "Regulating AI in Canada: a critical look at the proposed *Artificial Intelligence and Data Act*", (The Canadian Bar Review, 2023, Vol 101, No. 1), online: <https://cbr.cba.org/index.php/cbr/article/view/4817/4539>

The author analyzes the AIDA, the context in which it was tabled, and offers recommendations for improvements. The author reveals several deficiencies with the AIDA, including how its focus is on high impact AI systems yet the term "high impact" is not defined in the legislation, and how the striking feature of the AIDA is that so much is left to be defined in regulations, it appears devoid of substantive content and as a regulatory 'blank cheque'. The author examines what is "agile" regulation and finds that agility is not about relying on regulations but rather about supporting regulators in a more flexible, responsive, and data driven regulatory practice.

The paper also examines international AI governance initiatives, including the risk-based approaches taken in the EU in the context of the EU AI Act and the United States with its NIST AI risk management framework. The author notes how, under the AIDA, both the

Minister and Data Commissioner are responsible for the AIDA's enforcement, yet both positions are also located within the department charged with supporting innovation and economic development, raising questions about independence. The AIDA also excludes or overlooks groups and communities, focussing only on individuals and only on quantifiable harms. The author critiques the government for the lack of consultation on the AIDA and concludes by recommending that it be scrapped and that a proper AI consultation be initiated.

32. Scassa, Teresa, "Canada's Draft AI Legislation Needs Important Revisions", (Centre for International Governance Innovation, August 2023), online: [https://www.cigionline.org/articles/canadas-draft-ai-legislation-needs-important-revisions/?utm\\_source=cigi\\_newsletter&utm\\_medium=email&utm\\_campaign=ukraines-reconstruction-can-inform-the-wests-digital-transformation](https://www.cigionline.org/articles/canadas-draft-ai-legislation-needs-important-revisions/?utm_source=cigi_newsletter&utm_medium=email&utm_campaign=ukraines-reconstruction-can-inform-the-wests-digital-transformation)

The author argues that AI technology evolves so rapidly, it requires an agile regulatory response, but that AIDA is a rushed and problematic law. The author details five critiques of AIDA, stating they can all be addressed through a revision. The author states that while the government describes its approach to AI regulation as "agile", AIDA leaves much of the law to be articulated in regulations, which are not agile, since regulations often take longer than anticipated to develop and, in some cases, fail to ever materialize. The author notes that AIDA is meant to regulate high-impact AI systems, but that the definition of "high-impact" is left to future regulations. AIDA does not designate an independent regulator, and omits a broader concept of harm, such as systemic discrimination or environmental harm, limiting its current definition of "harm" largely to quantifiable harms to individuals. The author also critiques the government's lack of overall vision to AI governance and regulation.

33. Scassa, Teresa, "Proposed Data Privacy Law Favour Industry Over Individuals", (Toronto Star, October 7, 2022), online: <https://www.thestar.com/opinion/contributors/2022/10/07/proposed-data-privacy-law-favour-industry-over-individuals.html>

The author uses the metaphor of Blanche DuBois from "A Streetcar Named Desire" to demonstrate a critique of **Bill C-27**, namely that it **facilitates data use without adequate protections, which does not build trust in data practices**, leading to the potential for exploitation resulting from the reliance on "the kindness of strangers."

*The following blog posts, written by Dr. Teresa Scassa, are a series of posts about Bill C-27, the reform to Canada's private sector privacy law. These posts examine certain provisions of the Consumer Privacy Protection Act (CPPA) and the Artificial Intelligence and Data Act (AIDA), offering insights and analysis of the impact of the proposed legislation.*

34. Scassa, Teresa, "Bill C-27's Take on Consent: A Mixed Review", (July 4, 2022), online: [https://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](https://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)

This post examines Bill C-27 and compares it to former Bill C-11, the former privacy modernization Bill which died on the order paper prior to the last federal election in 2021. Specifically the post analyzes the difference in the consent provisions and what is changed and new in Bill C-27. The author notes that while Bill C-27 takes steps to address the concerns of both privacy advocates and those from industry with a series of revisions, **there is not much that is changed from former Bill C-11.**

35. Scassa, Teresa, "Anonymization and De-identification in Bill C-27", (July 4, 2022), online:  
[https://www.teresascassa.ca/index.php?option=com\\_k2&view=item&id=356:anonymization-and-de-identification-in-bill-c-27&Itemid=80](https://www.teresascassa.ca/index.php?option=com_k2&view=item&id=356:anonymization-and-de-identification-in-bill-c-27&Itemid=80)

This post looks at the anonymization and de-identification provisions found in Bill C-27, comparing its provisions to those found in former Bill C-11, Loi 25 and the regime under PIPEDA. The author states that the changes in Bill-27 reflect the power of industry lobbying, since there are two separate definitions for anonymized and de-identified data, and that organizations will be pleased to have a separate category of "anonymized" data, which is outside of scope of the statute. The author also examines Bill C-27's definition of "de-identify", which refers to modifying data so that individuals cannot be *directly* identified, potentially resulting in the use of the data without knowledge or consent in certain circumstances, even though specific individuals might still be identifiable from those data sets. The author finds that **Bill C-27 has downgraded the definition of de-identification from former Bill C-11 and provided little or no guidance beyond "generally accepted best practices" to address anonymization.**

36. Scassa, Teresa, "Statutory MadLibs – Canada's Artificial Intelligence and Data Act", (July 20, 2022), online:  
[https://www.teresascassa.ca/index.php?option=com\\_k2&view=item&id=359:statutory-madlibs-%E2%80%93-canada%E2%80%99s-artificial-intelligence-and-data-act&Itemid=80](https://www.teresascassa.ca/index.php?option=com_k2&view=item&id=359:statutory-madlibs-%E2%80%93-canada%E2%80%99s-artificial-intelligence-and-data-act&Itemid=80)

This post employs the use of a MadLib to demonstrate **the many items left to the regulations in AIDA.**

37. Scassa, Teresa, "Bill C-27 and the erasable right of erasure", (July 18, 2022), online:  
[https://www.teresascassa.ca/index.php?option=com\\_k2&view=item&id=358:bill-c-27-and-the-erasable-right-of-erasure&Itemid=80](https://www.teresascassa.ca/index.php?option=com_k2&view=item&id=358:bill-c-27-and-the-erasable-right-of-erasure&Itemid=80)

This post explains the **right of erasure** - the right for individuals to ask an organization to dispose of the personal information it holds about them - within proposed Bill C-27. It notes that the right only applies in three circumstances and highlights potentially problematic exceptions including (i) where the disposal of information would have an undue adverse impact to the ongoing provision of a product or service, (ii) where information is scheduled to be disposed of in accordance with an organization's

information retention policy, and (iii) where requests for deletion are "vexatious or made in bad faith". It finds that **the balance in Bill C-27 leans towards the free flow of personal data rather than protecting privacy**. The post concludes that a right intended to give more control to individuals instead merely provides organizations numerous exceptions to side-step it.

38. Scassa, Teresa, "Data Sharing for Public Good: Does Bill C-27 Reflect Lessons Learned from Past Public Outcry?", (July 11, 2022), online: [https://www.teresascassa.ca/index.php?option=com\\_k2&view=item&id=357:data-sharing-for-public-good-does-bill-c-27-reflect-lessons-learned-from-past-public-outcry?&Itemid=80](https://www.teresascassa.ca/index.php?option=com_k2&view=item&id=357:data-sharing-for-public-good-does-bill-c-27-reflect-lessons-learned-from-past-public-outcry?&Itemid=80)

This post highlights provisions in Bill C-27, tailored to address the needs of government and the commercial data industry to access personal data in the hands of the private sector. It notes the enlarged scope of Bill C-27's statistics and research provision (s. 35), which could problematically allow market and voter profile research due to the removal of the term "scholarly". Similar concerns around scope accompany s. 39, which addresses the sharing of de-identified personal information for "socially beneficial purposes". The post identifies substantive guardrails introduced in Quebec's Loi 25 and suggests that these practices, including the requirement of a privacy impact assessment, should be included in Bill C-27. It concludes that **Bill C-27 facilitates use without adequately protecting privacy**, a cynical approach given the lack of trust in government stemming from the recent StatCan and PHAC data sharing controversies.

39. Scassa, Teresa, "Bill C-27 and Children's Privacy", (July 25, 2022), online: [https://www.teresascassa.ca/index.php?option=com\\_k2&view=item&id=360:bill-c-27-and-children%E2%80%99s-privacy&Itemid=80](https://www.teresascassa.ca/index.php?option=com_k2&view=item&id=360:bill-c-27-and-children%E2%80%99s-privacy&Itemid=80)

This post comments that Bill C-27 modestly responds to advocates' concerns about children's privacy. It notes that constitutional concerns regarding the age of majority may limit a stronger response. The post suggests that the explicit characterization of the data of minors as "sensitive", and the exclusion of limitations on the right of erasure for minors, represents an improvement over PIPEDA and the proposed former Bill C-11. It concludes that **Bill C-27 offers some enhancement to minors' data protection rights**.

40. Scassa, Teresa, "Bill C-27 and a human rights-based approach to data collection", (August 2, 2022), online: [https://www.teresascassa.ca/index.php?option=com\\_k2&view=item&id=361:bill-c-27-and-a-human-rights-based-approach-to-data-protection&Itemid=80](https://www.teresascassa.ca/index.php?option=com_k2&view=item&id=361:bill-c-27-and-a-human-rights-based-approach-to-data-protection&Itemid=80)

This post highlights that privacy is a human right, recognized in international instruments and given quasi-constitutional status by the Supreme Court of Canada. It explains that, unlike predecessor Bill C-11, Bill C-27 references the human rights basis for privacy in its preamble but considers it as merely a factor to take into account alongside innovation and regulatory burden. The post highlights potential effects of the disparities between the

approaches taken in Bill C-27 and the EU's GDPR and Quebec's Loi 25. It concludes that **privacy as a human right should represent the starting point of Canadian privacy laws and that while innovation is good, it cannot be at the expense of human rights.**

41. Scassa, Teresa, "Canada's Proposed AI and Data Act - Purpose and Application", (August 8, 2022), online:  
[https://www.teresascassa.ca/index.php?option=com\\_k2&view=item&id=362:canadas-proposed-ai--data-act-purpose-and-application&Itemid=80](https://www.teresascassa.ca/index.php?option=com_k2&view=item&id=362:canadas-proposed-ai--data-act-purpose-and-application&Itemid=80)

This post looks at the scope of AIDA, explaining some of its constitutional (division of powers) challenges, as found in the dual purposes of the AIDA legislation. The post states that AIDA does not apply to federal government institutions and certain national defence institutions, finding that there is no reason why non-military national defence uses of AI should not be subject to governance. The post also **points to the limitations of AIDA and critiques the amount of information that is left to be determined by the regulations, in particular, the definition of "high impact system"**.

42. Scassa, Teresa, "Regulated Activities and Data under Bill C-27's AI and Data Act", (August 15, 2022), online:  
[https://www.teresascassa.ca/index.php?option=com\\_k2&view=item&id=363:regulated-activities-and-data-under-bill-c-27s-ai-and-data-act&Itemid=80](https://www.teresascassa.ca/index.php?option=com_k2&view=item&id=363:regulated-activities-and-data-under-bill-c-27s-ai-and-data-act&Itemid=80)

This post considers AIDA's activities and what data will be subject to governance under AIDA. It states that AIDA governs two categories of "regulated activity" so long as they are carried out "in the course of international or interprovincial trade and commerce". The post explains how these activities are cast in broad terms, and how the obligations in AIDA do not apply universally to all engaged in the AI industry. The post notes that, **how for many provisions, the details of what is actually required will depend upon regulations that have yet to be drafted.** It also highlights a comparison of the governance and oversight regime proposed in the CPPA and AIDA, noting how the CPPA offers oversight by an independent agent of Parliament, unlike AIDA.

43. Scassa, Teresa, "The Unduly Narrow Scope for "Harm" and "Biased Output" Under the AIDA", (August 22, 2022), online:  
[https://www.teresascassa.ca/index.php?option=com\\_k2&view=item&id=364:the-unduly-narrow-scope-for-harm-and-biased-output-under-the-aida&Itemid=80](https://www.teresascassa.ca/index.php?option=com_k2&view=item&id=364:the-unduly-narrow-scope-for-harm-and-biased-output-under-the-aida&Itemid=80)

This post **examines the unduly narrow scope for "harm" and "biased output" under AIDA.** It notes that the concept of harm is important to the AIDA framework and describes certain obligations on persons responsible for high-impact AI systems, such as the obligation to identify, assess, and mitigate risks of harm or biased output, and notify the responsible Minister in certain circumstances. The post also explains AIDA's oversight and enforcement functions, including the powers afforded to the Minister under AIDA. The post analyzes the use of the term "individual" in the definitions of harm in order to demonstrate the limitations of AIDA and examines the difference between the

use of the term "harm" and "biased output" under AIDA, noting that the definition of "harm" does not include "biased output".

44. Scassa, Teresa, "Oversight & Enforcement Under Canada's Proposed AI and Data Act", (August 29, 2022), online:  
[https://www.teresascassa.ca/index.php?option=com\\_k2&view=item&id=365:oversight-and-enforcement-under-canadas-proposed-ai-and-data-act&Itemid=80](https://www.teresascassa.ca/index.php?option=com_k2&view=item&id=365:oversight-and-enforcement-under-canadas-proposed-ai-and-data-act&Itemid=80)

This post explains that Bill C-27 creates new obligations for persons responsible for AI systems, particularly high impact systems, as well as those who process or make available anonymized data for use in AI systems. The author notes that the CPPA provides a suite of new enforcement powers that include powers to issue orders and impose administrative monetary penalties (AMPs) for non-compliance. The author examines the "teeth" and the "jaw" of the AIDA, noting that the **AIDA itself provides no mechanism for individuals to file complaints regarding any harms they may believe they have suffered, nor is there any provision for the investigation of complaints.** The post further critiques **the lack of independence from government in the oversight of AIDA** and analyzes the different routes for the imposition of AMPs or fines. The post concludes with a critique of **the lack of important details found in the AIDA concerning its oversight and enforcement scheme.**

45. Scassa, Teresa, "Regulating AI in Canada - The Federal Government and the AIDA", (October 11, 2022), online:  
[https://www.teresascassa.ca/index.php?option=com\\_k2&view=item&id=366:regulating-ai-in-canada-the-federal-government-and-the-aida&Itemid=80](https://www.teresascassa.ca/index.php?option=com_k2&view=item&id=366:regulating-ai-in-canada-the-federal-government-and-the-aida&Itemid=80)

This post looks at the federal government's constitutional authority to enact AIDA. Specifically, the author considers whether or not the federal government lacks the jurisdiction to regulate AI. The post also looks to other AI legal instruments in the European Union and the United States, as well as other policy frameworks for the use of AI

46. Scassa, Teresa, "Explaining the AI and Data Act", (March 21, 2023), online:  
[https://www.teresascassa.ca/index.php?option=com\\_k2&view=item&id=369:explaining-the-ai-and-data-act&Itemid=80](https://www.teresascassa.ca/index.php?option=com_k2&view=item&id=369:explaining-the-ai-and-data-act&Itemid=80)

This post considers whether ISED's March 13, 2023 companion document for AIDA addresses the many critiques of the bill as it was tabled by the government on June 16, 2022. The author concludes that ISED's document does not address these critiques and that a substantial rewrite of AIDA is necessary.

47. Scassa, Teresa, "Comparing the UK's proposal for AI governance to Canada's AI bill", (April 11, 2023), online:



[http://www.teresascassa.ca/index.php?option=com\\_k2&view=item&id=370:comparing-the-uks-proposal-for-ai-governance-to-canadas-ai-bill&Itemid=80](http://www.teresascassa.ca/index.php?option=com_k2&view=item&id=370:comparing-the-uks-proposal-for-ai-governance-to-canadas-ai-bill&Itemid=80)

The author compares the AIDA to the United Kingdom's consultation paper seeking input into its proposal for AI regulation, finding that the UK proposal and the AIDA are quite different. For example, the AIDA regulates high impact AI, which is left to be defined by the regulations of the AIDA, along with other essential elements. The AIDA also states that the Minister of Innovation is made generally responsible for its oversight and enforcement. The author notes that rather than create a new piece of legislation and/or a new regulatory authority, the UK proposal sets out five principles for responsible AI development and use. In the UK, existing regulators will be encouraged and, if necessary, specifically empowered, to regulate AI according to these principles within their spheres of regulatory authority. Examples of regulators who will be engaged in this framework include the Information Commissioner's Office, regulators for human rights, consumer protection, health care products and medical devices, and competition law. The UK scheme also accepts that there may need to be an entity within government that can perform some centralized support functions. These may include monitoring and evaluation, education and awareness, international interoperability, horizon scanning and gap analysis, and supporting testbeds and sandboxes. The author states that although Canada's federal government has labelled its approach to AI regulation as 'agile', the UK approach is much closer to the concept of agile regulation.

48. Scassa, Teresa, "Federal Court Dismisses Application for an Order against Facebook - and Raises Some Issues for PIPEDA Reform", (April 17, 2023), online: [https://www.teresascassa.ca/index.php?option=com\\_k2&view=item&id=371:federal-court-dismisses-application-for-an-order-against-facebook-and-raises-some-issues-for-pipeda-reform&Itemid=80](https://www.teresascassa.ca/index.php?option=com_k2&view=item&id=371:federal-court-dismisses-application-for-an-order-against-facebook-and-raises-some-issues-for-pipeda-reform&Itemid=80)

This post discusses the Federal Court of Canada case brought by the Privacy Commissioner of Canada against Facebook, in relation to the Cambridge Analytica scandal. The author states that the Federal Court dismissed the Privacy Commissioner's application largely because of a lack of evidence to establish that Facebook had failed to meet its PIPEDA obligations to safeguard its users' personal information. The author states that the Court chastised the Commissioner for its evidence gathering process, including the Commissioner's failure to use its statutory powers to compel evidence. The author also looks at how aspects of the decision should be deeply troubling to those concerned about privacy, such as the abandonment of the normative dimension of the concept of the reasonable expectation of privacy. **The author also states that some aspects of the decision should set off alarm bells with respect to Bill C-27, noting for example that information shared to third parties for socially beneficial purposes should include a safeguards requirement and that a human rights approach could provide a firm backstop when balancing commercial interests.** The author concludes by saying how bad law might also make bad cases and that the challenge will be to ensure that Bill C-27 does not reproduce or amplify deficiencies in PIPEDA.

49. Solove, Daniel J., "The Myth of the Privacy Paradox", (George Washington University Law School, 2020), online: [https://scholarship.law.gwu.edu/faculty\\_publications/1482/](https://scholarship.law.gwu.edu/faculty_publications/1482/)

The author examines the “privacy paradox” phenomenon where people say that they value privacy highly, yet in their behavior relinquish their personal data for very little in exchange or fail to use measures to protect their privacy. The author **deconstructs and critiques the privacy paradox and the arguments made about it.**

50. Travers Smith LLP, "Data Protection and Digital Information (no. 2) Bill" (March 17, 2023), online: <https://www.traverssmith.com/knowledge/knowledge-container/data-protection-and-digital-information-no-2-bill/>

The author reviews the key data protection reforms introduced by the U.K.'s Data Protection and Digital Information (No. 2) Bill (the "**Bill**"). The author argues that the Bill may be "a bit of a damp squib after October's rhetoric" and finds that the "risk of these reforms impacting the UK's adequacy seems slim". The author also notes that the expectation is that organizations already compliant with the current UK GDPR will not require changes to comply with the Bill.

51. Tesson, Christelle & Yuan Stevens, Momin M. Malik, Sonja Solomun, Supriya Dwivedi and Sam Andrey, "AI Oversight, Accountability and Protecting Human Rights: Comments on Canada's Proposed Artificial Intelligence and Data Act" (published in collaboration by the Cybersecure Policy Exchange at Toronto Metropolitan University, McGill University's Centre for Media, Technology and Democracy, and the Center for Information Technology Policy at Princeton University, November 2022), online: <https://static1.squarespace.com/static/5e9ce713321491043ea045ef/t/63614c030e02403d54fce254/1667320848453/AIDACommentary.pdf>

This report was collaboratively published by researchers at the Cybersecure Policy Exchange at Toronto Metropolitan University, McGill University's Centre for Media, Technology and Democracy, and the Center for Information Technology Policy at Princeton University. The authors make several recommendations to improve key concerns with AIDA. **The recommendations include:** (1) holding adequate public consultations on the AIDA with community advocates, researchers, lawyers, and groups representing the interests of BIPOC, 2SLGBTQIA+, economically disadvantaged, disabled and other equity-deserving populations; (2) that AIDA should be effectively regulated by an independent agent of Parliament with an independent tribunal to administer penalties in the event of a contravention; (3) that AIDA apply to government institutions; that the definition of AI be technologically neutral and future-proof, for example, focussing on the applications of AI instead of the techniques, and that the definition of AI be consistent across both the CPPA and AIDA; (4) that Bill C-27 address the human rights implications of AI systems in a comprehensive manner, for example, with prohibitions on processing biometrics such as facial recognition, subject to a limited set of exceptions; (5) that recourse be available in order to protect fundamental rights, such as the right to object to the automated processing of personal data, and the right to

appeal AI decisions; (6) that certain uses of AI be prohibited, for example, uses that exploit vulnerable groups or include social scoring; and that Bill C-27 and AIDA specifically include high levels of protection by default for children.

52. The White House (United States), "Blueprint for an AI Bill of Rights", October 2022, online: <https://www.whitehouse.gov/ostp/ai-bill-of-rights/>

The *Blueprint for an AI Bill of Rights* contains five guiding principles for the design, use, and deployment of automated systems that have the potential to meaningfully impact the American public's rights, opportunities, or access to critical resources or services. The White House states that the *Blueprint for an AI Bill of Rights* was developed through extensive consultation with the American public, and that its principles are a blueprint for building and deploying automated systems that are aligned with democratic values and protect civil rights, civil liberties, and privacy. The five guiding principles are: (1) safe and effective systems; (2) algorithmic discrimination protections; (3) data privacy; (4) notice and explanation; and (5) human alternatives, consideration, and fallback. The AI Bill of Rights includes a [Foreword](#), the five principles, [notes on Applying the Blueprint for an AI Bill of Rights](#), and guidance called, [From Principles to Practice](#).

53. Witzel, Mardi, "A Few Questions About Canada's Artificial Intelligence and Data Act", CIGI, August 11, 2022, online: <https://www.cigionline.org/articles/a-few-questions-about-canadas-artificial-intelligence-and-data-act/>

This article critiques the proposed AIDA by pointing out that AI industry-defining questions (such as what is a "high-impact system" and what constitutes "material harm") are left for future regulations and **the overarching governance arrangement in AIDA is foundationally flawed**: specifically, a single Ministry (ISED) is responsible both for drafting the law and associated policy and for administering and enforcing it (contrary to longstanding OECD Guidance that stresses the importance of regulatory decision-making independent from the political process).

54. Wylie, Bianca, "ISED's Bill C-27 + AIDA. Part 1: Tech, Human Rights, and the Year 2000", (October 9, 2022), online: <https://biancawylie.medium.com/iseds-bill-c-27-aida-part-1-tech-human-rights-and-the-year-2000-947088823f4e>

The author examines AIDA and portions of Bill C-27 and looks at the history of the government's efforts to legislate AI in Canada. The article states that when the government first began talking about the need for PIPEDA in the late 1990s, a parallel process was initiated by the House of Commons Standing Committee on Human Rights and the Status of Persons with Disabilities (HURAD) that expressed privacy protection firmly in the human rights language of the Universal Declaration of Human Rights. HURAD argued that truly effective privacy protection can be sustained only if the value of privacy as a human right is given greater weight than the bureaucratic efficiencies and economic benefits of an unconstrained flow of personal information.

55. Wylie, Bianca, "ISED's Bill C-27 + AIDA. Part 4: Calling on Federal MPs For a Necessary Defense of Democratic Process", (April 21, 2023), online: <https://biancawylie.medium.com/iseds-bill-c-27-aida-part-4-calling-on-federal-mps-for-necessary-defense-of-democratic-process-3003572bc38e>

The author critiques the government's approach to AIDA as being undemocratic, calling ISED both the cheerleader and fearmonger for the AI industry. The author states that AIDA was not informed by any kind of broad or wide-scale public discussion, and that the general public, including the communities that are most impacted by the technologies, have had minimal access to informed conversations about AI. The author explains that most of the organizations and people calling to support AIDA are funded by ISED or reliant on the notion of AI as a legitimate topic for their professional livelihood, representing a very narrow set of vested interests, which are not representative of the whole story of the AI sector. The author also examines the recent emergency meeting of the Canadian Advisory Council on AI that was called by the Minister of ISED, MP Champagne, stating that shortly after this meeting a letter emerged calling on Members of Parliament to support the AIDA. The author states that the letter reflects a closed loop of chorus of voices and that the signed letter is not replacement for formally and properly engaging the broader public in talking about AI, cautioning that this level of insider influence on law-making is insidious to the democratic process, blocks the aperture of the conversation from being appropriately broad, and scares off and silences most of the public.

56. Wylie, Bianca, "We're in an AI hype cycle—can Canada make it a responsible one?", (Canadian Centre for Policy Alternatives, July 2023), online: <https://monitormag.ca/articles/were-in-an-ai-hype-cycle-can-canada-make-it-a-responsible-one/>

The author critiques the federal government for rushing to regulate AI and states that it should go back to the drawing board for AI legislation. The author notes that we should be talking about what public administrative ethics requires of the subject, and what general adequacy in law drafting looks like. The author critiques the government for its approach to the AIDA, stating that if what is being done with the AIDA is permissible to our elected officials, we have bigger technological and democratic problems to understand. The author finds that to deal with the social impacts of AI, we must construct an entirely different conversation than one that has a primary goal of expanding the Canadian AI industry. The author states that even if the AIDA were to be heavily edited and corrected, we won't be able to escape its founding intent: the broader goal of normalizing AI's use across all sectors of society.

57. Urban, Jennifer M. & Chris Jay Hoofnagle, "The Privacy Pragmatic as Privacy Vulnerable", (*CUPS, Carnegie Mellon University Security and Privacy Institute*, 2014), online: <<https://cups.cs.cmu.edu/soups/2014/workshops/privacy/s1p2.pdf>> .

The article states that **Alan Westin's privacy segmentation model is structurally flawed and**, regrettably, overly cited. According to Westin, approximately half the U.S. population is made up of individuals with a mid-level concern for privacy, known as "**privacy pragmatists**". This conclusion has been used to promote a choice-based privacy regime which is, conveniently, favourable to the major corporations which supported Westin's research. The article concludes that the privacy segmentation model **should be used sparingly, if at all**.

58. Young, David, "Non-Identifiable Information Under Bill C-27", (September 30, 2022), online: <http://davidyounglaw.ca/compliance-bulletins/non-identifiable-information-under-bill-c-27/>

The author examines Bill C-27's framework for non-identifiable information, finding that it aligns with analogous frameworks under the EU's GDPR, the amended Quebec law and proposals being considered for an Ontario privacy law and a reformed law in BC. The author points to several areas for improvement in the proposed Bill and states that **going forward, an important aspect of privacy laws will be providing a supportable framework for both non-identifiable information and ethical AI**.

59. Young, David, "OPC appeals Federal Court's Facebook decision not requiring it to change its privacy practices", ([davidyounglaw.com](http://davidyounglaw.com)), online: <https://davidyounglaw.ca/compliance-bulletins/opc-appeals-federal-courts-facebook-decision-not-requiring-it-to-change-its-privacy-practices/>

The author discusses the OPC's appeal of the Federal Court's decision not requiring Meta (formerly Facebook) to change its privacy policies and procedures that had led to the Cambridge Analytica data breach. The author examines the Federal Court's decision upon which the appeal is based, stating that it contains some problematic determinations regarding PIPEDA, as well as the nature of evidence required on a court application to enforce the OPC's findings. The article states that PIPEDA Principle 3 was misinterpreted as an over-arching qualification to the requirement to obtain meaningful consent, for example, finding that more than a "reasonable effort" is required to confirm that meaningful consent was obtained. The author also notes how the Court found that a plain reading of Facebook's policies was not sufficient to conclude that Meta failed to represent a reasonable effort to inform users of the potential uses of their data. The article compares the "reasonable person" standard articulated by the Court to the test under the *Competition Act*, which use an objective criterion that can be applied to a range of fact situations and different levels of sophistication or credulity.

## Links to Relevant Legislation

### Canada - Federal

60. 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*, First Session, Forty-fourth Parliament, June 2022, online:  
<https://www.parl.ca/DocumentViewer/en/44-1/bill/C-27/first-reading>
61. Canada's Anti-Spam Legislation (CASL), *An Act to promote the efficiency and adaptability of the Canadian economy by regulating certain activities that discourage reliance on electronic means of carrying out commercial activities, and to amend the Canadian Radio-Television and Telecommunications Act, the Competition Act, the Personal Information Protection and Electronic Documents Act and the Telecommunications Act*, S.C. 2010, c. 23, online: <https://laws-lois.justice.gc.ca/eng/acts/E-1.6/index.html>
62. *Canada Elections Act*, S.C. 2000, c. 9, online: <https://laws-lois.justice.gc.ca/eng/acts/e-2.01/>
63. *Competition Act*, R.S.C 1985, c. C-34, online: <https://laws.justice.gc.ca/eng/acts/C-34/index.html>
64. Former Bill C-11, *An Act to enact the Consumer Privacy Protection Act and the Personal Information and Data Protection Tribunal Act and to make consequential and related amendments to other Acts*, Second Session, Forty-third Parliament, November 2020, online:  
<https://www.parl.ca/DocumentViewer/en/43-2/bill/C-11/first-reading>
65. *Personal Information Protection and Electronic Documents Act*, S.C. 2000, c. 5, online:  
<https://laws-lois.justice.gc.ca/eng/acts/P-8.6/index.html>

### Canada - Provincial

66. *Alberta Personal Information Protection Act*, Chapter P-6.5, online: [https://kings-printer.alberta.ca/1266.cfm?page=P06P5.cfm&leg\\_type=Acts&isbncln=9780779831562&display=html](https://kings-printer.alberta.ca/1266.cfm?page=P06P5.cfm&leg_type=Acts&isbncln=9780779831562&display=html)
67. *British Columbia Personal Information Protection Act*, SBC 2003, Chapter 63, online:  
[https://www.bclaws.gov.bc.ca/civix/document/id/complete/statreg/03063\\_01](https://www.bclaws.gov.bc.ca/civix/document/id/complete/statreg/03063_01)
68. Quebec's Law 25 (formerly Bill 64) *An Act to modernize legislative provisions as regards the protection of personal information, being*

*An Act respecting the protection of personal information in the private sector (chapter P-39.1)* online:

<https://www.legisquebec.gouv.qc.ca/en/document/cs/p-39.1>

read together with Bill 64, *An Act to modernize legislative provisions as regards the protection of personal information* (the relevant provisions being sections 93-152) online:

<http://www2.publicationsduquebec.gouv.qc.ca/dynamicSearch/telecharge.php?type=5&file=2021C25A.PDF>

- > French administrative version online at *Loi sur la protection des renseignements personnels dans le secteur privé* (Act respecting the protection of personal information in the private sector) prepared by the Commission d'accès à l'information du Québec; and
- > English administrative version online at *Act Respecting The Protection Of Personal Information In The Private Sector* prepared by the Canadian law firm BLG.

## European Union

69. European Union, *Data Governance Act*, 2022, online: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32022R0868>
70. European Union *General Data Protection Regulation*, Regulation (EU) 2016/679, online: <https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:32016R0679>
71. European Union *Proposal for an Artificial Intelligence Act*, online: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52021PC0206>
72. European Union, *Whistleblower Directive*, Directive (EU) 2019/1937, online: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32019L1937>

## United Kingdom

73. United Kingdom, *Age Appropriate Design Code* (aka the *UK's Children's Code*), 2020, online: <https://ico.org.uk/media/for-organisations/guide-to-data-protection/key-data-protection-themes/age-appropriate-design-a-code-of-practice-for-online-services-2-1.pdf>
74. United Kingdom, *Data Protection Act*, 2018, online: <https://www.legislation.gov.uk/ukpga/2018/12/contents/enacted>
75. United Kingdom, *Data Protection and Digital Information (No. 2) Bill*, online: <https://commonslibrary.parliament.uk/research-briefings/cbp-9803/>

**United States**

76. United States, *American Data Privacy and Protection Act*, online: <https://www.congress.gov/bill/117th-congress/house-bill/8152/text>
77. United States, *Data Elimination and Limiting Extensive Tracking and Exchange Act* (the "DELETE Act") online: <https://www.congress.gov/bill/117th-congress/senate-bill/3627/text>
78. California, *The California Age-Appropriate Design Code Act*, 2022 online: [https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill\\_id=202120220AB2273](https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=202120220AB2273)
79. California, *The California Privacy Act of 2018*, online: <https://oag.ca.gov/privacy/ccpa>
80. California, *The California Privacy Act Regulations*, online: <https://oag.ca.gov/privacy/ccpa>
81. California, *Delete Act*, online: [https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill\\_id=202320240SB362](https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=202320240SB362)
82. Colorado, *Privacy Act*, 2021, online: <https://coag.gov/resources/colorado-privacy-act/>  
[https://leg.colorado.gov/sites/default/files/2021a\\_190\\_signed.pdf](https://leg.colorado.gov/sites/default/files/2021a_190_signed.pdf)
83. Connecticut, *Data Privacy Act*, 2022, online: <https://www.cga.ct.gov/2022/ACT/PA/PDF/2022PA-00015-R00SB-00006-PA.PDF>
84. Utah, *Consumer Privacy Act*, 2022, online: <https://le.utah.gov/~2022/bills/static/SB0227.html>
85. Virginia, *Consumer Data Protection Act*, 2021, online: <https://law.lis.virginia.gov/vacodefull/title59.1/chapter53/>

**United Nations**

86. *United Nations Declaration on the Rights of Indigenous Peoples* (UNDRIP), GA Res 61/295, online: <https://www.un.org/development/desa/indigenouspeoples/declaration-on-the-rights-of-indigenous-peoples.html>