



CENTRE FOR DIGITAL RIGHTS
CENTRE POUR LES DROITS NUMÉRIQUES

Not Fit For Purpose – Canada Deserves Much Better

Centre for Digital Rights' Statement
on Bill C-27

Canada's *Digital Charter Implementation*
Act, 2022

Octobre 28, 2022

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.

TABLE OF CONTENTS

	Page
Executive Summary	4
About the experts CDR consulted.....	6
A. Introduction	7
B. Recommendations to fix Bill C-27's problems and make it fit for purpose	8
1. <i>Make Bill C-27 fit for addressing current privacy challenges and consistent with contemporary global privacy standards</i>	8
2. <i>Frame the purposes of Bill C-27 properly</i>	9
2.1 Recognize privacy as a fundamental human right.....	9
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).....	10
3. <i>Address the privacy risks to democracy</i>	10
3.1 Expressly extend the CPPA to cover Canada's federal political parties (FPPs).....	10
4. <i>Recognize the serious privacy risks to groups as well as to individuals</i>	11
4.1 Extend privacy protection to mitigate risks to groups.....	11
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.	11
4.3 Protect minors with special, enhanced privacy requirements.....	12
4.4 Clearly specify certain no-go zones as always being inappropriate purposes for collecting, using and/or disclosing an individual's PI.....	12
5. <i>Fix the consent provisions.</i>	12
5.1 Strengthen valid consent in section 15 of the CPPA by restoring the "understanding" requirement in section 6.1 of PIPEDA.	12
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.....	13
5.3 Eliminate implied consent as an alternative to the express consent basis for permitted collection, use or disclosure of PI.....	13
6. <i>Use all the tools in the "privacy and consumer protection toolbox" to promote accountability</i>	13
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, and when the processing is likely to result in a high risk to individuals' rights and freedoms. 14

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"). 14

6.3 Promote the development of data stewardship models. 14

6.4 Strengthen security safeguards. 15

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. 15

6.6 Adopt a more comprehensive regime governing third party data processors/service providers. 15

6.7 Clearly impose transparency and accountability obligations on data brokers..... 16

7. *Strengthen individuals' control over their PI*.....16

7.1 Provide for a more comprehensive right to PI "mobility" (aka "portability")..... 16

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. 16

7.3 Strengthen information and access. 17

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"). 17

7.5 Give individuals the rights to contest and object to ADS/AI affecting them, not just a right to "algorithmic transparency"..... 17

7.6 Strengthen the private right of action (PRA)..... 18

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. 19

8. *Give the Privacy Commissioner more teeth and bite*.....19

8.1 Scrap the proposed Personal Information and Data Protection Tribunal. 19

8.2 Provide for more flexible enforcement..... 20

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.20

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)..... 20

8.5 Strengthen the inter-agency collaboration and information-sharing provisions between the Privacy Commissioner, the Commissioner of Competition, and the CRTC. 21

8.6 Strengthen the whistleblowing regime. 21

8.7 Implement a self-reporting program for organizations..... 22

9. *Send Artificial Intelligence and Data Act (AIDA) back to the drawing board*.....22

9.1 AIDA is improper and incomplete. 22

9.2 AIDA inappropriately focuses excessively on risks of harms to individuals to the exclusion of collective harms..... 22

9.3 AIDA possesses contradictory language and fragile enforcement powers. 23

9.4 AIDA inappropriately focuses on an overly narrow range of algorithmic techniques23

C. Summary and Conclusion24

Appendix "A" - Other recommendations to strengthen Bill C-27.....25

10.1 Hold directors and officers personally liable..... 25

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. 25

Appendix "B" - Recommendations for further study.....26

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 26

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. ... 27

11.3 Provide the Office of the Privacy Commissioner with sufficient funding for it to properly fulfill its mandate..... 29

11.4 Protect the complainant's confidentiality and anonymity throughout the complaint process, including judicial reviews and appeals31

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..... 33.

Appendix "D" - Busting the myth that stricter privacy regulation stifles innovation37

Appendix "E" – Annotated bibliography.....39

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.

In consultation with some of Canada's leading privacy experts and thought leaders, the Centre for Digital Rights (**CDR**) has prepared this Statement 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 Statement 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 premature (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 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.

- 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.
- 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.
- 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.
- **AIDA should be sent back to the drawing board**. It is improper and incomplete, and inappropriately focuses excessively on risks of harms to individuals rather than on 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

Dr. Colin Bennett

Colin Bennett is Professor of Political Science at the University of Victoria, British Columbia. 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 has recently been appointed the first-ever scholar-in-residence at Office of the Information and Privacy Commissioner of Ontario. 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 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"](#). Unfortunately, the current bill does no better overall. 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 personal information 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 personal information (**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.

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 Statement 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 premature (AIDA) legislation.

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 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), some sections of which came into force on September 22, 2022, 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. 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 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.

We understand that Canadian officials have been given private assurances that both Bill C-11, and presumably Bill C-27, meet this bar of "essential equivalence". Canada should not be so confident. Noted below 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 Statement 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, 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.

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

Unlike 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.

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 "consumers".

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, 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 for has recently [found](#) that FPPs are subject to British Columbia's Personal Information Protection Act.

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.

The CPPA gestures at minors' needs for privacy protections by calling their PI "sensitive" but 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 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* and the September 2022 *California Age-Appropriate Design Code Act*).

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:

The consent of the 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.

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 privacy impact assessment (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.

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, and when the processing is likely to result in a high risk to individuals' 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 "C".

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 socially beneficial 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.

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.**

Akin to Bill C-11, 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 personal information 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 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 data flows entirely within Canada and those from Canada to another country and provide for stricter privacy protections for personal data 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 came into force on June 23, 2022 and will be applicable as of September 1, 2023), a fiduciary duty to individuals should be imposed on data processors who act as intermediaries between individuals and data collectors to ensure that such service providers only use PI entrusted to them for the purposes intended by the individuals.

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 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 that have been proposed in the European Commission's April 2021 *Proposal for a Regulation Laying Down Harmonized Rules on AI* (the **EU AI Act**). These proposed rules include (1) a ban on ADS/AI systems used to manipulate human behaviour, to exploit information about individuals or groups, to carry out social scoring, or to conduct indiscriminate surveillance and (2) a requirement that remote biometric identification systems used in public places, like facial recognition, would need special authorization from privacy protection authorities.

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 to the right to an 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.

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.

***Note:** 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.

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 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. **Send Artificial Intelligence and Data Act (AIDA) back to the drawing board**

AIDA is simply not ready and needs further consultation to tackle the demands of today and tomorrow.

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.

Promises 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

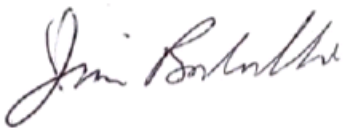
algorithmic amplification of divisive, hateful, sensationalist or politically manipulative messaging, which do not necessarily depend on the small set of sophisticated, novel techniques listed in its definition of AI.

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. Bill C-27 does not align with contemporary global standards or the current reality of personal data flows.

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 Statement 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
Centre for Digital Rights, Founder

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.

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 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 recently 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.¹ 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 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 4th quarter of

1. Based on Net cash provided by Government in the OPC's annual reports. See latest report [here](#).

2020.² In Canada, it costs an advertiser on average over US\$1 for a single user clicking on a Google ad.³ 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.⁴ 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

2. See Statista's chart: *Facebook's average revenue per user as of 4th quarter 2020, by region* [here](#).

3. See Wordstream's *Average Cost per Click by Country* [here](#).

4. [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.

11.4 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")
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

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, and when the processing is likely to result in a high risk to individuals' 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. Send the *Artificial Intelligence and Data Act (AIDA)* back to the drawing board

- 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

(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 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. Lev-Aretz and Strandburg's research led them to conclude that "across-the-board assertions about the stifling effects of information privacy regulation on innovation are simply wrong."⁵

In contrast to such broad assertions, scholars support the position that privacy regulation may impact innovation, but such impact depends on the regulatory design.⁶ For example, Goldfarb and Tucker's research suggests that privacy regulation may affect the extent and direction of data-based innovation, however, the impacts of privacy regulation can be extremely heterogeneous.⁷ 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.⁸ Aridor, Che and Salz's research⁹, which examined the impact of the GDPR on an online travel intermediary, supports the position that regulation impacts businesses but is not guaranteed to stifle or harm business interests.¹⁰

CDR is strongly of the view that rigorous fairness, accountability and transparency rules for ADS do not stifle innovation. It does the opposite. Instilling trust in individuals with respect to the potential innovative uses of their data, whether it be personally identifiable or anonymized, will encourage innovation.

In May 2021, the United Kingdom's Taskforce on Innovation, Growth and Regulatory Reform (**UK Taskforce**)¹¹ published an independent report (the **TIGRR Report**)¹² concerning

⁵ 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.

⁶ *Ibid.*

⁷ Avi Goldfarb and Catherine E. Tucker, *Privacy and Innovation*, Innovation Policy and the Economy (2012) 12, online <https://doi.org/10.1086/663156>.

⁸ 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).

⁹ 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).

¹⁰ 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.

¹¹ 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.

¹² 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

recommendations to the UK Prime Minister on how the UK can reshape its approach to regulation to drive innovation, growth and competitiveness. As a result of its consultation, the UK Taskforce recommends 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 maintains that regulation of the modern economy, including the digital economy, can encourage competition, stimulate innovation, and promote economic growth while concurrently protecting consumers and workers.¹³

The UK Taskforce notes 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."¹⁴

Further, the UK Taskforce notes that a lack of regulation can in fact stifle innovation and investment. In its report, the UK Taskforce maintains 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.¹⁵

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 recommends that it is appropriate in certain instances to promote innovation through new standards and rules tailored specifically to SMEs and new market entrants¹⁶ and it recognizes 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".¹⁷

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.

¹³ *Ibid.*, at 12.

¹⁴ *Ibid.*, at 5.

¹⁵ *Ibid.*, at 28.

¹⁶ *Ibid.*, at 6.

¹⁷ *Ibid.*

Appendix "E"

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 Statement. 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 Sectar, 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/

The 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. Balkin, Jack M., "The Fiduciary Model of Privacy", (*Harvard Law Review*, November 2020), online: 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.

3. 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.

4. 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.**

5. 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.

6. 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.

7. 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.

8. 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.

9. 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*.

10. 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.

11. 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/

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/

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.

12. 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/

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).

13. 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.

14. 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

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.**

15. 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

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.**

16. 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%93canada%E2%80%99s-artificial-intelligence-and-data-act&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 employs the use of a MadLib to demonstrate **the many items left to the regulations in AIDA.**

17. 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

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.

18. 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

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.

19. 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

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.**

20. 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

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.**

21. 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

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".**

22. 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

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.

23. 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

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".

24. 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

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.**

25. 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

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.

26. Solove, Daniel J., "The Myth of the Privacy Paradox", (George Washington University Law School, 2020), online: 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.**

27. 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).

28. 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.

29. 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**.

30. 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**.

Links to Relevant Legislation

31. 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>
32. 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>
33. *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>
34. European Union *General Data Protection Regulation*, Regulation (EU) 2016/679, online:
<https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:32016R0679>
35. European Union *Proposal for an Artificial Intelligence Act*, online:
<https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52021PC0206>
36. 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>

Unfortunately, no official government consolidation is yet publicly available. However, please see the unofficial/administrative

> French 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 version online at [*Act Respecting The Protection Of Personal Information In The Private Sector*](#) prepared by the Canadian law firm BLG.
37. British Columbia *Personal Information Protection Act*, SBC 2003, Chapter 63, online: https://www.bclaws.gov.bc.ca/civix/document/id/complete/statreg/03063_01
38. 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
39. 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>
40. California, *The California Age-Appropriate Design Code Act*, 2022 online: https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=202120220AB2273