CENTRE FOR DIGITAL RIGHTS
CENTRE POUR LES DROITS NUMÉRIQUES

Not Fit For Purpose - Canada Deserves Much Better

SUMMARY OF REPORT

Centre for Digital Rights' Report on Bill C-27
Canada's *Digital Charter Implementation Act, 2022*

October 2, 2023

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.

Summary of Report[1]

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

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 It is critically important for Canadian businesses that the adequacy judgment is not rescinded.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

Canadians also care about their privacy. In a recent survey[2], 93% of Canadians expressed concerns about the protection of their privacy. Fewer Canadians believe that businesses are respecting their privacy rights, and only 1 in 10 Canadians trust social media companies to protect their personal information.

In consultation with some of Canada's leading privacy experts and thought leaders[3], the Centre for Digital Rights (**CDR**) has prepared a Report on Bill C-27 (of which this document is a summary), recommending to **make Bill C-27 fit for addressing Canada's current privacy challenges and consistent with contemporary global privacy standards.** This Report aims to assist in the vital task of remediating the deficiencies of Bill C-27, by drawing on Canada's history of privacy innovation and examples from leading jurisdictions elsewhere. It offers specific recommendations for making the proposed CPPA fit for current and future challenges and highlights the concerns of rushing unnecessary (PIDPTA) and inadequate (AIDA) legislation.

As set forth in the Appendix to this Summary, CDR's October 2, 2023 Report makes over 40 recommendations to fix Bill C-27 and make it fit for purpose. Of these, CDR's key recommendations 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

[1] The full Report is available at https://www.centrefordigitalrights.org/our-work/canada-privacy-regulation
[2] Office of the Privacy Commissioner of Canada, *2022-23 Survey of Canadians on Privacy-Related Issues*, March 2023 https://www.priv.gc.ca/en/opc-actions-and-decisions/research/explore-privacy-research/2023/por_ca_2022-23/
[3] In preparing this Report, CDR consulted mainly with Professors Teresa Scassa, Colin Bennett and Andrew Clement.

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. The federal government's recent amendment of the *Canada Elections Act* purporting to provide a uniform and exclusive approach to how the FPPs protect Canadians' privacy is both hypocritical and a violation of the *Constitution of Canada* ("**Canada's Constitution**") and the *Canadian Charter of Rights and Freedoms* (the "**Charter**"). In separate prepared remarks to the Senate Standing Committee on Legal and Constitutional Affairs on May 3, 2023, this amendment (when it was just a proposal) was described by both the Privacy Commissioner of Canada and Canada's Chief Electoral Officer as inadequate to protect Canadians' personal information and falling short of their recommendations for meaningful privacy obligations on the FPPs.

- The federal government should **consult meaningfully with Indigenous Peoples** and **recognize Indigenous data sovereignty**. Its failure to do so is inconsistent with the federal government's obligation to implement the *United Nations Declaration on the Rights of Indigenous Peoples*. It is unacceptable and inexcusable, especially in light of the well-established and well-known First Nations Principles of OCAP®. Indigenous voices must not be left out if the federal government is serious about building a foundation of trust in the digital world in Canada.

- Privacy protection should be extended to **recognize the privacy risks to groups as well as to individuals**. The CPPA should extend protection to groups that are sufficiently defined such as households and children in a classroom. "Sensitive information" should be appropriately defined in the statute and minors should be better protected with special, enhanced privacy requirements.

- The CPPA requires a **fix to the consent provisions**, since the CPPA has eliminated important consent language from PIPEDA and omitted the guardrails necessary to ensure adequate privacy protections that clearly rank the individual's interests and fundamental rights above the commercial interests of the organization. Express, opt-in consent should be sought on digital media for the collection, use or disclosure of personal information for purposes beyond what is necessary to provide a product or service. This form of consent should be unbundled from the terms of use, and not made a condition of providing the product or service. Sections 15 and 18 (re: legitimate interest) of the CPPA should be rewritten.

- The CPPA should **use all the tools in the "privacy and consumer protection toolbox" to promote accountability**. This includes requiring privacy impact assessments (**PIAs**) in advance of the use of invasive technologies or high-risk processing, stipulating privacy-by-default requirements, promoting the development of data stewardship models, additional requirements surrounding cross-border data flows, and a more comprehensive regime governing third party data processors/service providers.

- The CPPA should **strengthen individuals' control over their personal information** (**PI**), for example, by providing a more comprehensive right to data mobility (or portability) and limiting the exceptions to the right to disposal of PI.

- The CPPA should **give the Office of the Privacy Commissioner more teeth and bite.** The CPPA should equip the Privacy Commissioner with more flexible enforcement approaches as well as the power to impose administrative monetary penalties. The PIDPTA should be scrapped. No justification (privacy law innovation or otherwise) has been given for such a tribunal. Its assigned role and composition raise serious concerns (including unnecessary complexity, delay and uncertainty for both individuals and organizations in the resolution of a complaint). Further, there is no privacy law regime in the world (including the modern and progressive regime in the EU, as well as the regimes in California, Utah, Colorado, Virginia and Connecticut, and the proposed *American Data Privacy and Protection Act*) that has established a tribunal like the Tribunal being proposed under the PIDPTA. Nor is such a tribunal proposed in the Australian Government's February 16, 2023 Privacy Act Review Report 2022 .

- AIDA should be sent back to the drawing board, but not to ISED alone. It is improper and incomplete, and inappropriately focuses excessively on risks of harms to "individuals" rather than on risks of harms to "groups and communities" (also known as "collective" harms).

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

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

(i) Fixing and Making Fit Bill C-27

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

2. Frame the purposes of Bill C-27 properly

2.1. Recognize privacy as a fundamental human right

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

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

3. Address the privacy risks to democracy

3.1. Expressly extend the CPPA to cover Canada's federal political parties

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

4.1. Extend privacy protection to mitigate risks to groups

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

4.3. Protect minors with special, enhanced privacy requirements

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

5. Fix the consent provisions

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

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

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

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

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

5.6. Revise sections 15, 16 and 18 of the CPPA to address the concerns with the consent provisions raised in recommendations 5.1 through 5.5, above.

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

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

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

6.3. Promote the development of data stewardship models

6.4. Strengthen security safeguards

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

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

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

7. Strengthen individuals' control over their PI

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

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

7.3. Strengthen information and access

7.4. Prohibit, subject to specific and narrow exceptions, organizations from using automated decision systems (ADS)/artificial intelligence (AI) to collect, use or disclose an individual's PI to align with GDPR, Article 22 (to help ensure "adequacy")

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

7.6. Strengthen the private right of action

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

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

8.1. Scrap the proposed Personal Information and Data Protection Tribunal

8.2. Provide for more flexible enforcement

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

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

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

8.6. Strengthen the whistleblowing regime

8.7. Implement a self-reporting program for organizations

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

9.1. AIDA is improper and incomplete

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

9.3. AIDA possesses contradictory language and fragile enforcement powers

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

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

(ii) Strengthening Bill C-27

10.1 Hold directors and officers personally liable

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

(iii) For further study

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

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

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

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

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