CANADIAN
CIVIL LIBERTIES
ASSOCIATION

ASSOCIATION
CANADIENNE DES
LIBERTES CIVILES

# Submission to the Standing Committee on Industry and Technology regarding Bill C-27, An Act to enact the Consumer Privacy Protection Act, the Personal Information and Data Protection Tribunal Act and the Artificial Intelligence and Data Act and to make consequential and related amendments to other Acts

**Canadian Civil Liberties Association**
Daniel Konikoff | Interim Director – Privacy, Technology & Surveillance Program
Tashi Alford-Duguid | Staff Lawyer
Noa Mendelsohn Aviv | Executive Director and General Counsel

September 12, 2023

Canadian Civil Liberties Association
124 Merton St., Suite 400
Toronto, ON M4S 2Z2
Phone: 416-363-0321
www.ccla.org

Executive Summary....3
Recommendations Summary....4
Introduction....6
The Consumer Privacy Protection Act....6
  Privacy as a Fundamental Right....6
  Defining Information, Both Personal and Sensitive....7
  Ensuring Businesses Do No Harm....8
  Reframing Consent in a Digital Age....9
Artificial Intelligence and Data Act....11
  Harm....12
    Privacy as a Human Right....12
    Group Harm and Bias....13
  Regulations....14
    High-impact Systems....15
    Biased Output....16
  Gaps....16
    Independence....17
    Transparency....17
    Limited Application....18
Towards a New AI Regime for Canada....19
Appendix: CCLA’s petition, “AI Regulation Needs to Put Human Rights First”....21

# Executive Summary

The right to privacy is essential to Canadian democracy. The Canadian Civil Liberties Association ("CCLA") believes that the right to privacy safeguards individuals' rights and freedoms in the face of rapid technological change. Unfortunately, Canadian legislation and enforcement mechanisms have not kept up with advancements in AI and related technologies. Bill C-27 is no better: it inappropriately frames people's privacy rights as something to be balanced against and placed below commercial interests. Bill C-27 fails to capture the complexity of the harms and risks that AI can bring to bear on individuals, communities, and their fundamental rights.

In this submission, CCLA speaks to Bill C-27, the *Digital Charter Implementation Act*. This submission speaks briefly to the *Consumer Privacy Protection Act* (CPPA) and the *Personal Information and Data Protection Tribunal Act* (PIDPTA) before making an extended submission about the proposed *Artificial Intelligence and Data Act* (AIDA). Regarding the CPPA, CCLA recommends that Parliament amend the bill to recognize privacy as a fundamental human right, legislate stronger protections for personal information deemed sensitive, and improve concerning provisions that underplay individual consent and the harms that stem from reckless and non-consenting collection, use, and disclosure of personal information. Regarding PIDPTA, CCLA recommends substantial amendments that increase the Tribunal's independence and transparency.

With respect to AIDA, CCLA strongly recommends that Parliament amend the Act's most essential features to better protect human rights and civil liberties in Canada. AIDA should be amended to uphold privacy as a fundamental human right and to recognize the violation of privacy as a very real, very consequential harm. AIDA should also be amended to strengthen protections against AI's biased outputs that can adversely harm marginalized groups. AIDA is also incomplete and opaque: it leaves lynchpin components of its legislation—like the definition of "high-impact systems"—to be determined in regulations. CCLA calls for amendments to legislate these features *now*, rather than regulate them *later*.

It is also important that AIDA be amended to plug its many gaps that compromise democratic accountability, including AIDA's lack of an independent regulator and its underdeveloped transparency requirements for the use and management of AI systems. Given the questionable relationship between the public sector and private corporations in the public sector's use of AI, CCLA also recommends expanding AIDA's purview beyond the private sector so it may regulate the national security and public safety bodies that use AI in their everyday operations. And seeing as how much AI has already changed since Bill C-27 was first put before Parliament (look no further than the emergence of generative AI and ISED's new code of practice),[1] CCLA recommends AIDA be amended to enshrine periodic Parliamentary reporting and review so that AIDA may be given a fighting chance to keep up with technological development.

Our recommendations for Bill C-27 stress the importance of fundamental rights and freedoms to privacy legislation, and how these rights and freedoms should be protected in our shifting technological landscape. The CCLA has extensive expertise on data privacy and AI, and we would be happy to discuss these issues in the context of Bill C-27 with the INDU Committee.

[1] ISED. (August 16, 2023). "Canadian Guardrails for Generative AI – Code of Practice." *ISED*. https://ised-isde.canada.ca/site/ised/en/consultation-development-canadian-code-practice-generative-artificial-intelligence-systems/canadian-guardrails-generative-ai-code-practice

## Recommendations Summary

**RECOMMENDATION 1:** Revise Bill C-27's Preamble and amend section 5 (Purpose) of the CPPA to explicitly recognize privacy as a fundamental human right.

**RECOMMENDATION 2:** Amend the definition of "personal information" in section 2(1) to clarify what information specifically qualifies as personal information, such as *names, ID numbers, location data, online identifiers,* or *"factors specific to [a person's] physical, physiological, genetic, mental, economic, cultural or social identity."*

**RECOMMENDATION 3:** Section 2(1) should be amended to include a subcategory of "sensitive personal information" that specifically includes *health data, financial data, ethnic and racial origins, political opinions, religious beliefs, genetic data, biometric data,* and *sexual orientation*.

**RECOMMENDATION 4:** Remove s. 12(2)(b) and (c) of the CPPA, which could allow businesses to elide individual consent if collecting, using, or disclosing data represents a "legitimate business need."

**RECOMMENDATION 5:** Amend section 12(2)(d) to remove "at a comparable cost and with comparable benefits."

**RECOMMENDATION 6:** Remove section 12(2)(e) to ensure that businesses do not violate individuals' privacy rights when violations will "benefit" the business.

**RECOMMENDATION 7:** Remove section 18(2)(d) to eliminate the "any prescribed activity" consent exemption.

**RECOMMENDATION 8:** Remove section 18(3) in its entirety for it once again supposes an inappropriate balance between privacy rights and "legitimate business interests."

**RECOMMENDATION 9:** Amend section 75(f) to remove "in any other prescribed circumstance" so that the statute creates clear definitions and rights-respecting restrictions around how businesses use de-identified information.

**RECOMMENDATION 10:** Amend the *Personal Information and Data Protection Tribunal Act* to prioritize independence, transparency, and due process. This includes revising 6(1) to revoke the Minister of Industry's ability to recommend tribunal members; removing 15(4)(a) and (b) and amending the language of 15(4) to clearly state that the Tribunal requires a judicial order if they wish to keep a ruling private on grounds of the ruling disclosing confidential information; and removing section 21 to allow for appeals of Tribunal decisions to a relevant court.

**RECOMMENDATION 11:** Amend section 4 (Purpose) to explicitly recognize privacy as a fundamental human right.

**RECOMMENDATION 12:** Amend section 5(1) to expand AIDA's definition of *harm* to align with the EU's *AI Act* and to account for both "material or immaterial" harms built around normative and human-centred values, namely threats to privacy rights, dignity, and autonomy.

**RECOMMENDATION 13:** Amend section 5(1) to expand AIDA's definition of *harm* to include group harms against a collective. Add "biased output" as a harm in and of itself.

**RECOMMENDATION 14:** Remove "without justification" from the definition of *biased output* contained in section 5(1).

**RECOMMENDATION 15:** Amend section 5(1) to provide a definition of *high-impact systems* that regards *high-impact* in terms of an AI system's potential for material and immaterial risks and harms, in line with international standards. Expand the definitions to include "unacceptable systems," "limited-impact systems," and "low high-impact systems," consistent with the EU's *AI Act*, and establish similar conformity assessment procedures and transparency safeguards for limited and lower-impact AI systems.

**RECOMMENDATION 16:** Remove section 36(a) which can allow to regulators to define what constitutes justification for AI's biased output.

**RECOMMENDATION 17:** Amend section 13 through 21 (Ministerial Orders) to include provisions for an independent regulator or for sharing oversight of these orders with the Office of the Privacy Commissioner of Canada.

**RECOMMENDATION 18:** Amend sections 7 to shift the responsibility of assessing whether an AI system is high impact to an independent third-party assessor.

**RECOMMENDATION 19:** Amend section 11 pertaining to "Publication of description" of an AI system to require transparency obligations for all AI systems. These transparency requirements can be modelled upon the EU's *AI Act*'s transparency obligations for lower-risk systems. These obligations can include providing an explanation of how an AI system arrived at its decisions, as well as information on the data used to train the system and the accuracy of the system.

**RECOMMENDATION 20:** Remove section 3(2) on the Act's non-applicability to national security actors.

**RECOMMENDATION 21:** Amend section 4 (Purpose) of the Act to expand beyond regulating the use of AI in "international and interprovincial trade and commerce" to include the use of AI in the public sector, with mention of national security and public safety actors.

**RECOMMENDATION 22:** Amend language throughout the bill—including the name of Part 1, "Regulation of Artificial Intelligence Systems in the Private Sector"—to account for public sector and national security actors.

**RECOMMENDATION 23:** Amend AIDA to add periodic Parliamentary review and annual reporting so AIDA can keep abreast of rapid technological developments.

# Introduction

The Canadian Civil Liberties Association ("CCLA") is an independent, national, non-governmental organization that was founded in 1964 with a mandate to defend and foster the civil liberties, human rights, and democratic freedoms of all people across Canada. Our work encompasses advocacy, research, and litigation related to the criminal justice system, equality rights, privacy rights, and fundamental constitutional freedoms. Working to achieve government transparency and accountability with strong protections for personal privacy lies at the core of our mandate.

CCLA believes that the right to privacy is essential to Canadian democracy. Rights do not exist in a vacuum; the right to privacy is a gateway right to all other fundamental rights, and without a right to privacy, all other rights suffer. In particular, CCLA believes that the right to privacy safeguards individuals' *Charter* rights in the face of rapid changes in technology. Canadian legislation and enforcement mechanisms do not currently suffice to keep up with rapid advancements in AI and related technologies. AI technologies, ranging from human resources AI to facial recognition software, pose serious and evolving threats to Canadians' rights, and Bill C-27 does not resolve these concerns.

In this submission, CCLA speaks to Bill C-27, the *Digital Charter Implementation Act*. This submission addresses the *Consumer Privacy Protection Act* (CPPA) and the *Personal Information and Data Protection Tribunal Act* (PIDPTA) before making an extended submission about the *Artificial Intelligence and Data Act* (AIDA)—strongly recommending that Parliament substantially amend the Act to better protect human rights and civil liberties in the face of technological innovation. C-27's Preamble states its intent to "modernize Canada's legislative framework so that it is suited to the digital age," but in its current form, C-27 is at risk of lagging behind the times before it can meet the present.

Stronger, rights-driven governance around AI is not only something that advocacy groups want; the public wants it, too. In July, CCLA launched a petition calling for AI governance that puts human rights first.[2] The petition amassed over 6,500 signatures from individuals across the country, and we are appending the petition to this submission to show how much these issues resonate with the people upon which these technologies will have the most impact.

# The Consumer Privacy Protection Act

## Privacy as a Fundamental Right

While it is laudable that government consulted with civil society regarding the CCPA, the CPPA fails to take up one of civil society's chief concerns about the Act: it does not recognize privacy as a fundamental human right in need of additional legal protections. Privacy is a long-held Canadian value, interpreted through the *Canadian Charter of Rights and Freedoms* as freedom from unreasonable search and seizure. Privacy also enjoys quasi-constitutional status, one recognized by the Supreme Court of Canada as a prerequisite to other *Charter*-protected rights.[3] Current privacy laws, however, are by and large data protection statutes which do not

[2] Canadian Civil Liberties Association. (July 2023). "AI Regulation Needs to Put Human Rights First." CCLA Petition. https://takeaction.ccla.org/support-ai-regulations-canada

[3] Office of the Privacy Commissioner of Canada. (2019). "Privacy Law Reform – A Pathway to Respecting Rights and Restoring Trust in Government and the Digital Economy." Reports to Parliament on Canada's federal privacy laws. https://www.priv.gc.ca/en/opc-actions-and-decisions/ar_index/201819/ar_201819/

capture the complexities of privacy beyond issues of consent, access, and transparency.[4] And in the big data age in which we live, commercial entities wield tremendous powers to collect and use data, especially compared to the limited power people have to control how their personal information is collected and used. When commercial entities—who increasingly rely on monetizing personal information—hold more control over individuals' personal information than individuals do, those commercial entities may believe they have the power to decide that economic interests are more important than individuals' personal interest in privacy.

This is what the CPPA does: it enshrines finding a "balance" between individual privacy against commercial interests and allows commercial interests to win. This is inappropriate, and individual privacy should—and must—prevail over commercial interests.

Bill C-27 in general, and the CPPA in particular, need to define privacy in a consistent manner and make it an effective right. The Bill's Preamble speaks in broad terms about privacy's status as a threshold or gateway value that is "essential to individual autonomy and dignity and to the full enjoyment of fundamental rights and freedoms in Canada." This is an important sentiment that recognizes privacy *interests*, but it stops short of concretely calling privacy a right. The Preamble also declares that the Act aims "to support the Government of Canada's efforts to foster an environment in which Canadians can seize the benefits of the digital and data-driven economy and to establish a regulatory framework that supports and protects Canadian norms and values, including the right to privacy." Unfortunately, however, this right to privacy is not explicitly mentioned in the substance of the CPPA itself and thus remains unlegislated in the Act.

**RECOMMENDATION 1: Revise Bill C-27's Preamble and amend section 5 (Purpose) of the CPPA to explicitly recognize privacy as a fundamental human right.**

## Defining Information, Both Personal and Sensitive

"Sensitive information" remains undefined in Bill C-27. Parliament should follow international standards and explicitly define sensitive information to better protect special categories of personal information. Bill C-27 defines "personal information" as "information about an identifiable individual." According to the European Union's (EU) General Data Protection Regulation (GDPR), personal information includes names, ID numbers, location data, online identifiers, or "factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity" of a person.[5]

A lot of personal information is *sensitive*. The degree to which information qualifies as sensitive often depends on context, but there are special categories of information whose collection, use, or disclosure inevitably carries specific risks. Information considered sensitive under the GDPR includes health and financial data, ethnic and racial origins, political opinions and religious beliefs, genetic and biometric data, and sexual orientation.[6]In Canada, sensitive information is not explicitly codified under PIPEDA, so it fell to the Office of the Privacy

[4] Ibid.

[5] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) [2016] OJ L 119/1.

[6] European Commission. (2016). "What Personal Data is Considered Sensitive?" https://commission.europa.eu/law/law-topic/data-protection/reform/rules-business-and-organisations/legal-grounds-processing-data/sensitive-data/what-personal-data-considered-sensitive_en

Commissioner of Canada to issue guidance to businesses on how to better interpret information sensitivity and how to offer safeguards commensurate with information's sensitivity.[7]

"Sensitivity" is a concept that appears often throughout the CPPA, yet it remains undefined in the Bill's glossary of terms. Bill C-27 should follow the global standard for data protection and explicitly define *sensitive information* to capture the above-mentioned special categories. Failing to do so leaves far too much up to interpretation, and businesses might not take sensitive information as seriously as they should. This can lead businesses to establish inadequate protections (or no protections at all) for information that merits stronger safeguards, therefore putting personal privacy at risk. And without a definition for sensitive information, other sections—such as 53(2) and 62(2)(e), which refer to retention periods for sensitive personal information, or 57(1), which pertains to establishing safeguards proportionate to the sensitivity of the information—are left open to interpretation. This can leave privacy rights vulnerable, as sensitive information does not receive the explicit legislative protections its sensitivity requires. In short, not all personal information is sensitive, but all sensitive information is personal, and Parliament should amend Bill C-27's definitions to better clarify this reality.

**RECOMMENDATION 2: Amend the definition of "personal information" in section 2(1) to clarify what information specifically qualifies as personal information, such as *names, ID numbers, location data, online identifiers,* or *"factors specific to [a person's] physical, physiological, genetic, mental, economic, cultural or social identity."***

**RECOMMENDATION 3: Section 2(1) should be amended to include a subcategory of "sensitive personal information" that specifically includes *health data, financial data, ethnic and racial origins, political opinions, religious beliefs, genetic data, biometric data,* and *sexual orientation*.**

## Ensuring Businesses Do No Harm

Section 12 of the CPPA contains consent exemptions that inappropriately put the interests of businesses above those of individuals. Sections 12(1) and (2) of the CPPA state that "An organization may collect, use or disclose personal information only in a manner and for purposes that a reasonable person would consider appropriate in the circumstances, whether or not consent is required under this Act." Section 12(2) outlines "factors that must be taken into account in determining whether the manner and purposes referred to in subsection (1) are appropriate," and includes, on top of "(a) the sensitivity of the personal information," "(b) whether the purposes represent legitimate business needs of the organization." What an organization's "legitimate business needs" are, however, are unclear. Private business interests might at times conflict with the interests of individuals and consumers, and what may qualify as "legitimate business needs" to those in charge of a business may constitute a privacy violation or risk to consumers.

Section 12 also asks businesses to consider "whether the individual's loss of privacy is proportionate to the benefits in light of the measures...implemented by the organization to

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

mitigate impacts of loss of privacy on the individual." This once again puts the job of evaluating whether a business practice is worth the privacy risks onto businesses themselves, leaving companies to potentially prioritize their fiduciary duties to company interests over individuals' privacy rights.

**RECOMMENDATION 4: Remove s. 12(2)(b) and (c) of the CPPA, which could allow businesses to elide individual consent if collecting, using, or disclosing data represents a "legitimate business need."**

**RECOMMENDATION 5: Amend section 12(2)(d) to remove "at a comparable cost and with comparable benefits."**

**RECOMMENDATION 6: Remove section 12(2)(e) to ensure that businesses do not violate individuals' privacy rights when violations will "benefit" the business.**

## Reframing Consent in a Digital Age

Sections 18 through 28 of the CPPA legislate exceptions to requirements for consent, many of which pose problems for privacy. For example, s. 18(1) states:

> "An organization may collect or use an individual's personal information without their knowledge or consent if the collection or use is made for the purpose of a business activity described in subsection (2) and **(a)** a reasonable person would expect the collection or use for such an activity; and **(b)** the personal information is not collected or used for the purpose of influencing the individual's behaviour or decisions."

Further, section 18(2) defines business activities in relation to subsection (1) as: "**(a)** an activity that is necessary to provide a product or service that the individual has requested from the organization; **(b)** an activity that is necessary for the organization's information, system or network security; **(c)** an activity that is necessary for the safety of a product or service that the organization provides; and **(d)** any other prescribed activity."

These provisions are an affront to *meaningful consent*, the cornerstone of privacy. People should be able to meaningfully consent—or decline to consent—to how private companies gather and handle their personal data. But in our modern digital age, achieving that meaningful consent has become all the more challenging, with commercial entities wielding disproportionate powers of data collection and use compared to those of individuals. Businesses that collect, use, and disclose personal data without proper safeguards run the risk of breaching people's trust and violating their right to privacy in the process.

As written, these sections may lead organizations to misuse an individuals' personal information without their knowledge or consent. For example, section 18(2)(d)'s "any other prescribed activity" creates unnecessary room for abuse and should be removed from the legislation entirely. Further, there is often a disconnect in what meaningful consent means to individuals in light of how they make sense of data collection and data use, in which some instances of data collection and use are clear (like getting someone's address for shipping a product), while some instances are not (like sharing collected data with third-party buyers or using collected data to build customer profiles for advertising purposes). Relatedly, section 18(3) allows for organizations to collect personal information without an individual's knowledge or consent “if the collection or use is made for the purpose of an activity in which the organization has a legitimate interest that outweighs any potential adverse effect on the individual resulting from that collection or use.” It is unclear how the Act defines “legitimate interest,” and in the case of corporations, “legitimate interest” may be taken to mean “maximizing profit.” Once again, the CPPA allows for businesses—not consumers, not government, or anyone else—to determine whether their own interests outweigh any harms that may befall real people.

Further, section 75(f), outlines conditions under which businesses are permitted to use de-identified information, containing overbroad language permitting businesses to use this information “in any other prescribed circumstance.” The Bill does not define what a “prescribed circumstance” is, there are currently no regulations to give it substance, and even if there were, these regulations are too readily changed. This undermines people’s ability to provide corporations with meaningful consent and does not provide adequate protection against the potential abuse of individuals’ personal and de-identified information.

In sum, it is often unclear why and what data is being collected, how that data is being used, and how a company’s collection and use of data fits in with their broader business interests. When it comes to how companies use data, the language in the CPPA—“business activity”—is too unclear to effectively protect individuals’ rights to privacy. As written, section 18 provides companies too much leeway to bypass acquiring meaningful consent so long as they are pursuing their own business interests.

**RECOMMENDATION 7: Remove section 18(2)(d) to eliminate the “any prescribed activity” consent exemption.**

**RECOMMENDATION 8: Remove section 18(3) in its entirety for it once again supposes an inappropriate balance between privacy rights and “legitimate business interests.”**

**RECOMMENDATION 9: Amend section 75(f) to remove “in any other prescribed circumstance” so that the statute creates clear definitions and rights-respecting restrictions around how businesses use de-identified information.**

## The Personal Information and Data Protection Tribunal Act

In CCLA’s view, PIDPTA is at odds with transparent and effective approaches to regulating privacy rights because the proposed Personal Information and Data Protection Tribunal is not independent. The government cannot expect the public to place its trust in any administrative tribunal that is not independent, and for the Tribunal to be structured as anything less than independent runs the risk of private, corporate, and political capture.

Specifically, PIDPTA allows the Minister of Industry to recommend individuals for Tribunal membership, blurring the boundaries between those responsible for the Act and those enforcing it. PIDPTA also allows for private hearings away from the public eye if it deems certain hearings, per section 15(4)(a) “not...in the public interest.” These hearings would be comprised of bureaucrats appointed by the Minister, not independent judges or independent officers at an arms-length from Parliament. Further, per section 21, these important decisions would not even be eligible for appeal. CCLA strongly urges Parliament to amend the PIDPTA portion of Bill C-27 so it aligns with principles of good governance and due process: if the

Tribunal is to play a role in regulating and enforcing the privacy issues at stake in the CPPA, the Tribunal should do so independently and transparently.

**RECOMMENDATION 10: Amend the *Personal Information and Data Protection Tribunal Act* to prioritize independence, transparency, and due process. This includes revising 6(1) to revoke the Minister of Industry's ability to recommend tribunal members; removing 15(4)(a) and (b) and amending the language of 15(4) to clearly state that the Tribunal requires a judicial order if they wish to keep a ruling private on grounds of the ruling disclosing confidential information; and removing section 21 to allow for appeals of Tribunal decisions to a relevant court.**

## Artificial Intelligence and Data Act

The CCLA believes that the proposed *Artificial Intelligence and Data Act* (AIDA) threatens the right to privacy in Canada. Specifically, we believe that AIDA prioritizes commercial interests over fundamental rights, and that if Parliament is not going to scrap AIDA entirely, then it must heavily amend its most problematic features.

The power and danger of AI and algorithmic technologies should not be underestimated and must not be regarded as only a problem for legislators, policy wonks, or the business community. AI and algorithmic technologies have already been unlawfully deployed against communities and it is likely that AI will never again be as amenable to considered, resilient, and human rights-respecting regulation than it is today. The fastest way for Canada to get the laws we need is for Parliament to do what it must to get these laws right the first time. Canada cannot afford an AI law that, like the CPPA, establishes a framework for businesses to balance (and prioritize) commercial interests against individuals' fundamental rights and freedoms: the law must always put an individual's human right to privacy, personal autonomy, and human dignity first.

The rest of this submission focuses on three critical aspects of the proposed legislation, discussed through a privacy and rights-based lens: harm, regulation, and legislative gaps.

- **Harm**: AIDA should expand its definition of harm to better capture the risks that AI poses for individual privacy and collective equality.
- **Regulation**: AIDA should not leave key definitions, such as definitions related to high-impact systems and biased output, to regulation. The lack of clarity in the legislation leaves it without necessary details and opens the door to potential privacy and equality violations.
- **Gaps**: AIDA fails to recognize and protect a fundamental right to privacy because it focuses exclusively on the private sector. Government institutions and law enforcement agencies are key AI stakeholders who must be brought into a shared or cognate regulatory framework.

Regardless of how this legislation is ultimately implemented, critical issues affecting individuals' human rights and fundamental freedoms must not be left on the table as problems to solve at another time. AI systems will develop in Canada one way or another; we must ensure that the law does so with a deep commitment to fundamental rights and freedoms, and in a way that is consistent with good governance and the rule of law.

## Harm

At the centre of AIDA is a narrow and restrictive definition of 'harm' that needs amendment to more accurately account for the complex harms AI can cause. AIDA defines harm as "(a) physical or psychological harm to an individual; (b) damage to an individual's property; or (c) economic loss to an individual". Whereas AIDA construes 'harm' in individualistic terms, focusing on physical and psychological harm to individuals and commercial loss, CCLA urges the Committee to reject this definition as inadequate and misguided. In this framework, commercial and economic interests may be given priority over protecting against other risks that should also be recognized as harms, including a) risks to privacy, autonomy, and human dignity, and b) group harms such as bias.

### Privacy as a Human Right

In our increasingly digital, interconnected, and AI-driven world, AIDA's definition of 'harm' is too narrow, only focusing on physical and psychological harms to individuals. This definition risks overcommitting AIDA to a framework that fundamentally struggles to comprehend the diversity and complexity of harms that may stem from the technology of the day. Law professor Margot E. Kaminski notes that there are issues with this perspective, as it risks devaluing harms that are harder (or impossible) to quantify, and that it can obscure normative values behind ostensibly objective 'scientific' decisions.[8] Specifically, Kaminski finds that this sort of perspective risks de-emphasizing rights-based harms, such as those to dignity or autonomy, as well as harms that are otherwise difficult to measure, such as emotional harms or harms to democratic society.

These kinds of harms—harms to privacy, autonomy, dignity, and equality—are endemic to AI, and AIDA is ill-positioned to prevent them, because AIDA does not define harm in a way that captures these important normative and harder-to-quantify harms. And although AIDA acknowledges the close relationship between AI and harm to individuals in its Preamble, the Act is nevertheless designed around commercial interests rather than the harms arising from violating individuals' fundamental rights and freedoms. Finally, while "privacy interests" are mentioned in Bill C-27's Preamble, the word "privacy," its protection as a right, and the harm that comes from violating privacy rights, do not appear at all in AIDA's substance. Consistent with our recommendations above, Parliament should amend AIDA to recognize **privacy as a fundamental human right,** building the Act around *people* rather than commercial uses and interests. This would guide AIDA's legislative development and appropriately foreground how AIDA and similar laws can be designed to protect against privacy-related harms.

CCLA submits that without an unavoidable commitment to protecting privacy as a human right, AIDA will inevitably become an instrument for mining, processing, and abusing personal information in Canada. And as we have seen, the existence and use of unregulated AI poses a direct threat to individuals' privacy rights in Canada. Clearview AI, for example, unlawfully collected 3 billion facial images by scraping them from social networking sites without users' consent. Canadian law enforcement agencies used Clearview AI across

[8] Kaminski, M. (April 2023). "The developing law of AI: A turn to risk regulation." *The Digital Social Contract: A Lawfare Paper Series*.

jurisdictions.[9] Cadillac Fairview collected 5 million photos of shoppers without those individuals' consent, using facial recognition technology to analyze customers' age and gender for unspecified business purposes.[10] Similar, comparable, or wholly new AI-based transgressions of fundamental rights should never occur again. Without proactive governance, the public can expect comparable invasions of—and harm towards—individuals' privacy, autonomy, and dignity.

It is not enough for C-27 to just acknowledge the importance of human rights and fundamental freedoms in its Preamble, and it is not enough for AIDA's companion document to just gesture toward existing human rights-related institutions within Canada such as the *Canadian Human Rights Commission*.[11] Compared to similar AI-related legislation, such as the European Union's (EU) proposed *Artificial Intelligence Act*,[12] Canadian AI and privacy legislation undervalues rights and freedoms and struggles to integrate human-centred values[13] and concrete protections into its proposed framework. What is more, the EU's proposed *AI Act* acknowledges that harm can be both "material or immaterial," applying as much to "public interests and rights" as it does to one's body, mind, and wallet.[14] Compared to the EU's proposed framework for AI, AIDA can function more as a tool for advancing commercial and economic interests rather than prioritizing the genuine harms that AI can cause to human rights and privacy.

**RECOMMENDATION 11: Amend section 4 (Purpose) to explicitly recognize privacy as a fundamental human right.**

**RECOMMENDATION 12: Amend section 5(1) to expand AIDA's definition of *harm* to align with the EU's *AI Act* and to account for both "material or immaterial" harms built around normative and human-centred values, namely threats to privacy rights, dignity, and autonomy.**

## Group Harm and Bias

AIDA defines harm exclusively on an individual level and disregards AI's role in causing group-based harms. By only codifying this individualistic conception of harm, AIDA fails to recognize the full spectrum of harms that can be caused with AI and algorithmic technologies. In a legal system that typically relies on quantitative evidence, it could be unduly difficult to demonstrate group or society-based harms and risks using only an individualistic framework.

[9] Office of the Privacy Commissioner of Canada. (June 10, 2021). "Police use of Facial Recognition Technology in Canada and the way forward." *OPC.* https://www.priv.gc.ca/en/opc-actions-and-decisions/ar_index/202021/sr_rcmp/
https://www.priv.gc.ca/en/opc-news/news-and-announcements/2020/nr-c_201029/

[11] Innovation, Science and Economic Development Canada. (March 2023). "The Artificial Intelligence and Data Act - Companion document." *Government of Canada.* https://ised-isde.canada.ca/site/innovation-better-canada/en/artificial-intelligence-and-data-act-aida-companion-document

[12] European Parliament. (April 2021). "Briefing - EU Legislation in Progress - Artificial Intelligence Act." "https://www.europarl.europa.eu/news/en/headlines/society/20230601STO93804/eu-ai-act-first-regulation-on-artificial-intelligence

[13] OECD Policy Observatory. (May 2019). "Human-Centred Values and Fairness (Principle 1.2)." *Organisation for Economic Co-operation and Development.* https://oecd.ai/en/dashboards/ai-principles/P6

[14] European Parliament. (April 2021). "Briefing - EU Legislation in Progress - Artificial Intelligence Act." "https://www.europarl.europa.eu/news/en/headlines/society/20230601STO93804/eu-ai-act-first-regulation-on-artificial-intelligence

One of the ways in which AI can contribute to group harms is by deepening racial discrimination, economic inequities, and other social biases. Although AI offers many practical and economic advantages, the algorithms and data upon which AI systems are built can still produce discriminatory and biased results, which risks harming people both inside and outside of Canada. For example, studies of AI used in facial recognition technologies often disproportionately target or misidentify members of racialized communities.[15] Use of AI can thereby amplify disparities between communities based on race, gender, and other grounds of discrimination prohibited by the *Charter* and human rights statutes across Canada.

Although AIDA incorporates the concept of biased output within the legislation's definitions, the concept is not put to good use. Specifically, AIDA's definition of biased output includes an exception that weighs whether an outcome that "adversely differentiates, directly or indirectly" towards a person based on prohibited grounds of discrimination has adequate justification. There are many problems here. First, the definition and purpose of the phrase "without justification" are currently not defined. Second, this definition does not acknowledge the harm that biased algorithmic decision-making can cause to both individuals and groups. And most important, it makes the inappropriate, unacceptable, and anti-rights suggestion that there are instances in which a biased output against a member of an equity-seeking group can be justified.

**RECOMMENDATION 13: Amend section 5(1) to expand AIDA's definition of *harm* to include group harms against a collective. Add "biased output" as a harm in and of itself.**

**RECOMMENDATION 14: Remove "without justification" from the definition of *biased output* contained in section 5(1).**

## Regulations

AIDA leaves many central issues up to regulations, including the definition for 'high-impact systems.' Definitions of key terms play a central role in AIDA as they inform which AI technologies and levels of harm are permissible within the Canadian private sector. Leaving definitions of key terms to regulations risks minimizing the strength of the legislation, since regulations are far easier to amend and exist largely at the will of the Governor in Council. Individuals, groups, and businesses would all benefit from having the fundamental elements of Canada's ultimate AI law codified in statute rather than regulations.

Some of those in Parliament are of the opinion that lacking regulations is a boon, drawing a false equivalence between "no regulations" and "agility." In a statement from the office of Minister of Industry Francois-Philippe Champagne, "C-27 would give the government a flexible framework to introduce industry standards and regulations that can evolve with this rapidly developing technology."[16] But this is misguided. When definitions of key terms are codified in legislation, legislators and civil society are given a better opportunity to scrutinize the scope and rationale of government decisions and contribute to their improvement.

[15] Najibi, A. (October 24, 2020). "Racial Discrimination in Face Recognition Technology." *Harvard University's Science in the News.* https://sitn.hms.harvard.edu/flash/2020/racial-discrimination-in-face-recognition-technology/

[16] Cnockaert, J. (May 3, 2023). "Legislation that keeps up with AI may require special committee with expert panel, says NDP critic." *The Hill Times.* https://www.hilltimes.com/story/2023/05/03/legislation-that-keeps-up-with-ai-may-require-special-committee-with-expert-panel-says-ndp-critic/385933/

However, when key aspects of the legislation are left to be decided through regulations, many legislators and civil society are largely screened out of the legislative process, which significantly limits opportunities for the scrutiny and second opinions which these regulations will require.

## High-impact Systems

AIDA's more stringent requirements around identifying, assessing, and mitigating risks of AI harms apply to what the Act refers to as 'high-impact systems,' but AIDA does not provide a definition of high-impact systems. Instead, it leaves the criteria for high-impact systems to be assessed in the regulations. Until such regulations are promulgated, anyone seeking to implement or be protected by the legislation may be left to speculate as to what "high-impact" means: is a system "high-impact" if it poses the most harm? Affects the most people? Is used by the highest number of businesses? As high-impact systems are a key target for this legislation, they should be clearly and transparently defined in the legislation from the start. For any major piece of legislation, clear and defined key terms are essential to making the legislation operational and effective. Without them, the law might be revised too readily by the government of the day, a vulnerability that is fundamentally at odds with reliable protection for human rights and civil liberties in Canada.

For this or any comparable legislation to be successful, it is essential to have a clear and transparent definition in the statute setting out the terms at the core of the legislation, especially for 'high-impact system.' To flesh out this concept, Parliament can look to the EU's *AI Act*, which provides a tiered template for proactively assessing AI systems based on their level of risk. Under the EU's *AI Act*, AI systems posing "unacceptable risk" are prohibited, `and include any AI systems that perform real-time and remote biometric identification, social scoring, or that manipulate the cognitive behaviour of people or vulnerable groups.[17] AI systems with "high risk" are permitted subject to both standing requirements and a conformity assessment, AI systems with "limited risk" are permitted so long as they meet transparency obligations, and AI systems with "minimal or no risk" are permitted without restrictions.[18] Overall, the EU's proposed legislation demonstrates that clarifying key concepts can strengthen legislation's effectiveness rather than limiting the legislation's ability to adapt with the technology.

Additional processes surrounding high-impact systems remain obscure because they are banished to regulation. Under AIDA, persons responsible for high-impact systems must establish measures to identify, assess, and mitigate the risks of harm or biased output that could result from the use of the system. These persons must also establish measures to monitor compliance with such mitigation measures. Yet the particulars of these measures are unclear; they are not part of the Act but are instead part of its unreleased regulations. The fundamental lack of transparency surrounding AIDA means that Parliament is not in a position to make significant and informed amendments to the law because, as it stands, there is hardly any law to amend—AIDA amounts to an expression of intent to make a law, rather than a clear plan to which parliamentarians, experts, civil society actors, and the public can all make fulsome response. Such a thin expression of intent is not enough around which to build a viable AI law, especially because this law must also safeguard fundamental rights and freedoms.

[17] European Parliament. (April 2021). "Briefing - EU Legislation in Progress - Artificial Intelligence Act." "https://www.europarl.europa.eu/news/en/headlines/society/20230601STO93804/eu-ai-act-first-regulation-on-artificial-intelligence

[18] European Commission. (2021). "Regulatory Framework Proposal on Artificial Intelligence." *EU.* https://digital-strategy.ec.europa.eu/en/policies/regulatory-framework-ai

By contrast, the EU's plan makes many more substantial commitments. For example, the EU's proposed approach to risk management would require that the highest-risk technologies, in addition to other safeguards, undergo conformity assessment procedures and be registered with a "declaration of conformity" before being put into use.[19] The EU's proposed standards also provide more safeguards which apply even if an AI system is of lower impact and risk, including a rule that individuals be reasonably notified when they are interacting with an AI system or that they are being exposed to other biometric recognition systems and deepfakes.[20]

**RECOMMENDATION 15: Amend section 5(1) to provide a definition of *high-impact systems* that regards *high-impact* in terms of an AI system's potential for material and immaterial risks and harms, in line with international standards. Expand the definitions to include "unacceptable systems," "limited-impact systems," and "low high-impact systems," consistent with the EU's *AI Act*, and establish similar conformity assessment procedures and transparency safeguards for limited and lower-impact AI systems.**

### Biased Output

As mentioned above, AIDA's definition of biased output includes an exception for biased output that contains "justification," but the legislation leaves the phrase undefined because, per section 36(a), it supposes that the issue of what qualifies as adequate justification for bias will be addressed in regulation. The inclusion of an exception for justification raises questions about the exception's purpose in the legislation and its role within Canada's broader legal framework for preventing and providing redress for discrimination. Further, the inclusion of this exception may open the door for private companies to disguise biased outputs with pre-approved "justifications." This can leave AIDA vulnerable to capture by commercial interests at the expense of the public's fundamental rights to privacy, dignity, and democratic accountability.

It is not sufficient for regulation to make up for omissions in legislation. Without more clarity in the legislation about the role of bias in AI, there is no guarantee in AIDA that individual privacy and human rights will guide and inform how the legislation is ultimately deployed. It is difficult to conceive of anything that can "justify" biased output, and AIDA should not give regulators the opportunity under section 36(a) to create exceptions that allow for AI to "justifiably" discriminate.

**RECOMMENDATION 16: Remove section 36(a) which can allow to regulators to define what constitutes justification for AI's biased output.**

## Gaps

In addition to the principled problems with AIDA identified above, the legislation also features considerable gaps with respect to independence, transparency, and applicability.

[19] Chatterjee, S. (August 7, 2023). "Conformity Assessments in the EU AI Act: What You Need to Know." *Holistic AI.* https://www.holisticai.com/blog/conformity-assessments-in-the-eu-ai-act#:~:text=Conformity%20assessments%20(CAs)%20are%20required,the%20legislation%20for%20AI%20systems.

[20] European Parliament. (April 2021). "Briefing - EU Legislation in Progress - Artificial Intelligence Act." "https://www.europarl.europa.eu/news/en/headlines/society/20230601STO93804/eu-ai-act-first-regulation-on-artificial-intelligence

## Independence

AIDA does not provide for an independent regulator, compromising any claims the Act can make to due process and democratic accountability. Oversight and enforcement of AIDA are provided by the same Ministry and Minister that drafted the law and that will draft its prospective regulations. This is not a mechanism for effective oversight so much as a blurred line between parliamentary action and executive decision-making—not transparent, not effective, and not in Canada's best interest.

The Act also grants corporations—not an independent regulator—the power to determine whether a business' AI systems are high impact or not. Since AIDA's toughest restrictions apply to high-impact systems, this provision raises concerns around whether corporations will identify their AI systems as high impact or if they will just use high-impact systems without identifying them as such. This would allow high-impact systems and the businesses that use them the opportunity to evade governance, posing a threat to individual and group privacy everywhere.

**RECOMMENDATION 17: Amend section 13 through 21 (Ministerial Orders) to include provisions for an independent regulator or for sharing oversight of these orders with the Office of the Privacy Commissioner of Canada.**

**RECOMMENDATION 18: Amend sections 7 to shift the responsibility of assessing whether an AI system is high impact to an independent third-party assessor.**

## Transparency

AIDA lacks essential transparency obligations for those who use or manage AI systems. AIDA contains two sections related to the publication of descriptions around high-impact AI systems. Under sections 11(1) and 11(2), those who "[make] available for use" or "[manage] the operation of" high-impact systems must "publish on a publicly available website a plain language description of the system that includes an explanation of" how the system is intended to be used; what types of content it will generate; what kind decisions, recommendations, and predictions it will make; and any mitigation measures put in place to minimize its harms. This is a good start, but it does not go far enough, for even those systems posing minimal risk or lower impact—whatever that may mean under AIDA—should be subject to transparency obligations.

Parliament must ensure that AI and algorithmic technologies are transparent, and that their use is made transparent to the public. Individuals have a right to know when their personal information is being used by today's increasingly inscrutable AI systems. In practice, this rule would include at least two elements: (1) meaningful notice of the use of algorithmic technologies and (2) the capacity to opt out of their use in decisions. For example: patients should be notified if their personal information is fed into an AI to make medical diagnoses, and artists should be given meaningful prior notice before their work is used to create AI-generated art. This transparency is necessary if these technologies—and those who use them—are ever going to be accountable for their policies and decisions, which is an essential component of any society which seeks to make responsible use of AI and algorithmic technologies.

Disclosing the use of AI to the public, however, does not cure all of AI's possible defects. AI is difficult for even experts to understand, a challenge which we anticipate will only grow more formidable over time. Making AI understandable to the public is thus both an essential part of any possible future for AI in Canada, as well as just the start of what the public should expect of a transparent process for developing and using AI and algorithmic technologies in Canada. After all, individuals cannot sue or otherwise make a complaint about a process if they cannot understand it—or if they are unaware that the technology is in play at all. Making AI public can help individuals better understand how AI affects their lives, and it can ensure that institutions are held accountable if AI systems pose risks to fundamental rights and freedoms.

**RECOMMENDATION 19: Amend section 11 pertaining to "Publication of description" of an AI system to require transparency obligations for all AI systems. These transparency requirements can be modelled upon the EU's *AI Act*'s transparency obligations for lower-risk systems. These obligations can include providing an explanation of how an AI system arrived at its decisions, as well as information on the data used to train the system and the accuracy of the system.**

## Limited Application

AIDA does not capture national security bodies under its legislative framework, allowing institutions with historically problematic uses of AI technology to continue evading governance for the often intrusive ways they use AI. Specifically, AIDA explicitly does not apply to the Minister of National Defence, the Director of the Canadian Security Intelligence Service, and the Chief of the Communications Security Establishment, nor does AIDA apply to Canadian law enforcement. Artificial intelligence technologies have become essential tools in national security and public safety, though recent abuses of these tools—such as the recent case of the misuse of facial recognition technology playing a role in Immigration, Refugee and Citizenship Canada revoking the refugee status of a Black woman from Africa—have spot-lit the dire need for their regulation.[21] And as was demonstrated by the ETHI Committee's study and report on the RCMP's use of on-device investigation tools, the privately acquired AI tools that public actors use can have tremendous consequences for privacy and human rights.[22]

This speaks to a broader gap that AIDA fails to address: the significance of public-private AI-related partnerships. AIDA's exclusive focus on the private sector disregards the role that public contracts play in developing private sector AI technology. Though CCLA acknowledges that there is precedent for separating privacy-related bills along public and private lines, those lines are far blurrier when AI is in the mix. The law's application might struggle to traverse these very uncertain boundaries, meaning there is little use in legislating them independently. Parliament should pay particular attention to the interconnection—and oftentimes questionable boundaries—between government action, government-funded actions, mixed public and private actions, wholly private actions, and public policy when it comes to AI. Without clear standards for demarcating these boundaries, the Committee should presume

[21] Christian, G. (August 22, 2023). "AI Facial Recognition Technology: The Black Box Hurting Black People." *Toronto Star*. https://www.thestar.com/opinion/contributors/ai-facial-recognition-technology-the-black-box-hurting-black-people/article_67c4a8e6-e377-55c6-9e63-2bd209e99dc3.html

[22] Brassard, J. (November 22). "Device Investigative Tools Used by the Royal Canadian Mounted Police and Related Issues." *ETHI*. https://www.ourcommons.ca/Committees/en/ETHI/StudyActivity?studyActivityId=11794265

that bodies could seek to interpret and utilize these boundaries for self-serving purposes and in direct contravention of human rights. AIDA can and must acknowledge the significance of public-private AI-related partnerships by reworking its non-application provisions, so it may bring better governance to the way Canada's national security and public safety apparatuses use AI.

**RECOMMENDATION 20: Remove section 3(2) on the Act's non-applicability to national security actors.**

**RECOMMENDATION 21: Amend section 4 (Purpose) of the Act to expand beyond regulating the use of AI in "international and interprovincial trade and commerce" to include the use of AI in the public sector, with mention of national security and public safety actors.**

**RECOMMENDATION 22: Amend language throughout the bill—including the name of Part 1, "Regulation of Artificial Intelligence Systems in the Private Sector"—to account for public sector and national security actors.**

## Towards a New AI Regime for Canada

Canada needs a robust and reliable framework for addressing the challenges posed by AI technologies, and AIDA is not it. The legal framework that Canada needs must begin with the fundamental premise that privacy is a human right, and it should not regard privacy as something that can be balanced against—and indeed ranked as less than—commercial interests. We need legislation that captures the complexity of risks and harms that AI poses, but that also puts individual and collective privacy interests first: privacy must be both the instrument and the objective for this and any future privacy-involving legislation. Corporate, commercial, and partisan interests must be reconciled with fundamental human rights. National security and law enforcement bodies too must be brought within the law's ambit.

We also need legislation that does not leave its most important features to undrafted regulations. Leaving such crucial components of AIDA to its regulations allows some of AIDA's most consequential provisions and definitions to evade the most rigorous democratic review and meaningful amendment. Casting such essential elements of legislation to be hashed out in regulation, away from the significant scrutiny these complex AI questions require, leaves an opening for commercial entities to use these consequential tools in ways that are antithetical to fundamental rights.

As AIDA progresses through Committee amidst larger cultural conversations about AI, it is likely that AI will continue to move faster than Parliament can keep up with. Parliament should add periodic Parliamentary review and reporting to this law, so that AIDA can keep abreast of rapid technological developments. While this may seem cumbersome, it is absolutely necessary to secure our fundamental rights against newer and potentially more inscrutable technologies.

**RECOMMENDATION 23: Amend AIDA to add periodic Parliamentary review and annual reporting so AIDA can keep abreast of rapid technological developments.**

AIDA needs amendment to align with the principles of good AI governance. Good AI governance stresses *legality*, in that technology should comply with applicable laws. Good AI governance stresses *fairness* and *consistency*, both operational and procedural: it should be bias-free, should be subject to audit and evaluation, and should apply to all who use AI, in every sector. Good AI governance will make sure that AI systems are *reliable, and* that their use is both *transparent* and *explainable*. Good AI governance will enforce *accountability* of those who make AI systems and the organizations that use them. Good AI governance protects *privacy* writ large. Good AI governance is not built in a vacuum, but is built from *meaningful engagement*, both with those who stand to win from AI and, more important, with those who stand to lose. Canada cannot afford AI regulations that do not take those very real losses—losses to privacy rights, losses to equality—into account.

# Appendix: CCLA's petition, "AI Regulation Needs to Put Human Rights First"

Petition can be accessed at: https://takeaction.ccla.org/support-ai-regulations-canada

Artificial intelligence (AI) poses risks to privacy and human rights. While concerns about a killer robot takeover might be far-fetched, AI is generating disinformation and threatening democracy, putting people out of work, and contributing to social inequalities through biased decision-making in sectors from healthcare to finance to criminal justice.

**The Artificial Intelligence and Data Act (AIDA) is one of Canada's first attempts at regulating AI. However, in its current form, AIDA puts economic development first, giving private sector interests priority over fundamental human rights.**

AIDA has problems. For one, AIDA was made with virtually no consultation, leaving out experts from civil society who best understand AI's ups and downs. AIDA doesn't define important concepts like 'high-impact AI' systems, making it hard to know which uses of AI the Act actually covers. AIDA doesn't apply to police and national security agencies, even though these agencies rely on worrisome AI tools that can be used for mass surveillance. AIDA also puts the oversight of AI into the hands of the same minister responsible for promoting AI innovation, which raises questions about whose interests—those of the private sector or those of the public—will take priority. **AIDA also doesn't treat 'biometric information'—like fingerprints, voice patterns, or facial features—as sensitive information worthy of special protection.** And most importantly, AIDA leaves essential features of the law up to future regulations, to be made only once the bill has been passed. Without an idea of AIDA's regulations, we're left to wonder how—or whether—AIDA will work at all.

**If AI is going to play any larger role in Canada, then we need laws that take it seriously:** Canada needs fit-for-purpose legislation that protects individuals and communities and that recognizes the risks AI poses for privacy and human rights.

**You have the power to make that happen.**

**Join us in calling on the Government of Canada to commit itself to do more to protect our fundamental rights in the face of AI's rapid development.** The rights and liberties that AI puts at risk cannot become afterthoughts in the pursuit of innovation.

Governments around the world are starting to regulate AI, from the European Union's AI Act to the United States' Blueprint for an AI Bill of Rights. **Canada's Parliament will study AIDA in Fall 2023, so we still have time to get AI laws right. Sign our petition now to demand revisions to AIDA that:**

1. Codify individuals' privacy as a priority over corporate and commercial interests;
2. Codify a definition of "high-impact" systems, and expand the definition of sensitive information to explicitly include biometric information;
3. Set out transparency and disclosure requirements for private businesses and public bodies to notify people when and how AI is in use;
4. Reallocate the oversight of AIDA compliance from the Minister of Innovation to the Office of the Privacy Commissioner of Canada;
5. Provide additional funding to the Office of the Privacy Commissioner of Canada to support its role in Canada's regulatory framework for AI;
6. Align Canada with international best practices, such as the OECD.AI principles of good governance and the European Union's AI Act;
7. Impose a moratorium on facial recognition technology (FRT) in Canadian industries until a robust regulatory framework is developed and implemented, consistent with the

recommendations outlined by Parliament’s Standing Committee on Access to Information, Privacy and Ethics’ (ETHI) from their report on FRT and the growing power of AI;

8. Increase transparency and oversight mechanisms for the use of AI in the context of national security and procurement, consistent with the recommendations outlined by Parliament’s Standing Committee on Access to Information, Privacy and Ethics’ (ETHI) from their report on FRT and the growing power of AI.

Letter addressed to:
To:
The Honourable Dominic LeBlanc, P.C., M.P., Minister of Public Safety
The Honourable François-Philippe Champagne, P.C., M.P., Minister of Innovation, Science and Industry
Joël Lightbound, Chair of the Standing Committee on Industry and Technology

CC:
The Honourable Michelle Rempel Garner, P.C., M.P., Parliamentary Caucus on Emerging Technology
The Honourable Colin Deacon, Senator, Parliamentary Caucus on Emerging Technology
Members of the Standing Committee on Access to Information, Privacy and Ethics
Members of the Standing Committee on Industry and Technology