NOVEMBER 2022

AI Oversight, Accountability and Protecting Human Rights:

Comments on Canada's Proposed *Artificial Intelligence and Data Act*

Christelle Tessono, Yuan Stevens, Momin M. Malik, Sonja Solomun, Supriya Dwivedi and Sam Andrey

cybersecure policy exchange Powered by RBC

CENTER FOR INFORMATION TECHNOLOGY POLICY PRINCETON UNIVERSITY

Centre for MEDIA, TECHNOLOGY and DEMOCRACY

Cybersecure Policy Exchange

The Cybersecure Policy Exchange (CPX) is an initiative dedicated to advancing effective and innovative public policy in cybersecurity and digital privacy through Rogers Cybersecure Catalyst and the Leadership Lab at Toronto Metropolitan University. Our goal is to broaden and deepen the debate and discussion of digital privacy and security policy in Canada, and to create and advance innovative policy responses. This initiative is sponsored by the Royal Bank of Canada; we are committed to publishing independent and objective findings and ensuring transparency by declaring the sponsors of our work.

@cyberpolicyx @cyberpolicyx Cybersecure Policy Exchange
For more information, visit: https://www.cybersecurepolicy.ca/

Center for Information Technology Policy at Princeton University

The Center for Information Technology Policy (CITP) at Princeton University is a nexus of expertise in technology, engineering, public policy, and the social sciences. In keeping with the strong University tradition of service, the Center's research, teaching, and events address digital technologies as they interact with society.

@PrincetonCITP
For more information, visit: https://citp.princeton.edu/

Centre for Media, Technology and Democracy at McGill University

Collaborating with a network of academic, policy, journalistic and community stakeholders, the Centre for Media, Technology and Democracy works to understand and address the democratic harms of emerging media technologies and to inform and develop fair and accountable governance systems. The Centre for Media, Technology and Democracy produces critical research, policy activism, and inclusive events that inform public debates about the changing relationship between media and democracy, and that ground policy aimed at maximising the benefits and minimizing the systemic harms embedded in the design and use of emerging technologies.

@MediaTechDem
For more information, visit: https://www.mediatechdemocracy.com/

Table of Contents

Executive Summary

This report is a collaboration of interdisciplinary researchers from the Cybersecure Policy Exchange at Toronto Metropolitan University, McGill University's Centre for Media, Technology and Democracy, and the Center for Information Technology Policy at Princeton University.[1]

Canada's investment in developing AI systems has not been matched by a comparable effort to regulate the technology. While we are encouraged by these initial efforts to regulate AI systems in Canada, we share several key concerns, with corresponding recommendations to improve the proposed framework, particularly under the *Artificial Intelligence and Data Act* (AIDA) of the newly tabled Bill C-27: *Digital Charter Implementation Act, 2022*.

Recommendations

1. **The Need for Adequate Public Consultation**
   Innovation, Science and Economic Development Canada should formally consult on AIDA with community advocates, researchers, lawyers, and groups representing the interests of BIPOC, 2SLGBTQIA+, economically disadvantaged, disabled and other equity-deserving populations in the country.

2. **The Need for Proper Oversight of AIDA**
   To effectively regulate the AI market in Canada, the AIDA Commissioner needs to be an independent agent of Parliament and we need to empower an independent tribunal to administer penalties in the event of contravention, outline best practices for auditing, and enforce the law as required.

3. **AIDA Must Apply to Government Institutions**
   Given that AIDA only currently applies to the federal private sector — as government institutions are explicitly exempt from AIDA — it is imperative that AIDA's framework be broadened to include government institutions.

4. **Bill C-27 Needs Consistent, Technologically Neutral and Future-Proof Definitions**
   Both the *Consumer Privacy Protection Act* (CPPA) and AIDA within Bill C-27 should provide for a definition of AI or algorithmic systems that is cohesive across both laws. The definition of AI ought to be technologically neutral and future-proof. A potential pathway for regulation is to define algorithmic systems based on their applications instead of focusing on the various techniques associated with machine learning and AI.

5. **Bill C-27 Must Address the Human Rights Implications of Algorithmic Systems**
   Bill C-27 needs to address the human rights risks of algorithmic systems in a comprehensive manner:

- This should include, but not be limited to, prohibitions on the processing of biometric data such as facial images through automated means for the unique identification of individuals, especially in public settings and potentially subject to a very limited set of exceptions.
- Bill C-27 and particularly AIDA need to provide people with recourse in order to protect fundamental rights when AI systems are used — such as the right to object to the automated processing of personal data, as well as the right to appeal decisions that are made when algorithmic systems are used.
- Certain uses of algorithmic systems (e.g., ones that exploit vulnerable groups based on age, physical or mental disabilities, or systems used by the state for social scoring purposes) must also not be allowed because they pose unacceptable risks to people's safety, livelihoods, and rights, which requires more than AIDA's current approach to identifying and managing risk.
- Bill C-27 and AIDA more specifically should also include high levels of protection by default for children.

1. The Need for Adequate Public Consultation

AIDA came as a surprise to the public: there were no public notices that it would be included in the new iteration of the *Digital Charter Implementation Act*. As noted by the Canada Research Chair in Information Law and Policy, Professor Teresa Scassa, there was only mention of the creation of a new Data Commissioner in the Budget 2021 and in the Minister of Innovation, Science, and Industry's mandate letter. However, neither had an articulation of the regulatory framework it would be part of.[2]

But more significantly, Bill C-27 did not have any public consultations. For AIDA, we are aware that a consultation with the government's AI advisory council took place.[3] However, there are no publicly accessible records accounting for how these meetings were conducted, nor which points were raised by the council. Innovation, Science, and Economic Development Canada (ISED) has recently hosted consultations on the *Innovation Canada Act*, on a *National Quantum Strategy*, and the regulatory modernization of the *Bankruptcy and Insolvency Act*.[4, 5] The absence of a thorough public consultation process for Bill C-27, and more specifically AIDA, demonstrate that effective mechanisms in place to hold consultations are not being used in order to draft critical legislation. Because AIDA regulation is set to be crafted by the the Minister of Innovation, Science and Industry,[6] consultations will be at their discretion. As a result, the risk for future regulation to not take into account the public and the voices of marginalized communities is a significant concern.

Public consultations are important as they allow a variety of stakeholders to exchange and develop innovative policy that reflects the needs and concerns of affected communities. As raised by economist and journalist Erica Ifill, the lack of meaningful public consultation — specifically with BIPOC, trans and non-binary, economically disadvantaged, disabled and other equity-deserving populations — is echoed by AIDA's failure "to acknowledge AI's characteristic of systemic bias including racism, sexism, and heteronormativity."[7] Moving forward, meaningful consultations related to this Act, privacy and AI more broadly, should be spearheaded with the values of equity, diversity, and inclusion in mind. This would enable greater interaction between technical experts, marginalized communities, and regulation.

Moreover, to hold effective public consultations, it is key to assess the different roles the Canadian government performs in the AI ecosystem. If certain departments serve as intermediaries for funding innovation within industry, which departments are then available to the public to influence and hold potentially harmful innovation to account? As raised by Mardi Witzel, associate at NuEnergy.ai, ISED is a government department that plays a key role in supporting technological innovation within industry. And in light of this, it is "reasonable to ask how a ministry that collaborates with and funds digital and AI-enabled industries can serve as an impartial enforcer of the design, development and use of this same technology by its constituent clients."[8]

Recommendations

- **Moving forward, ISED should facilitate a series of formal consultations on AIDA** with community advocates, privacy and AI ethics experts, technologists, lawyers, and groups representing the interests of BIPOC, 2SLGBTQIA+, economically disadvantaged, disabled and other equity-deserving populations in the country.
- As suggested by Erica Ifill, **ISED should release their GBA+ analysis of AIDA** in order to see how they considered the impact of the legislation on marginalized populations.[9]

2. The Need for Proper Oversight of AIDA

The AI Commissioner and Advisory Committee Are Not Enough

The proposed Artificial Intelligence and Data Commissioner is set to be a senior public servant designated by the Minister of Innovation, Science and Industry and is therefore not independent of the Minister. They will "assist the Minister in the administration and enforcement" of AIDA. Moreover at the discretion of the Minister, the Commissioner *may* be delegated the power, duty, and function to administer and enforce AIDA.[10] In other words, the Commissioner is not afforded the powers to enforce AIDA in an independent manner as their powers depend on the Minister's discretion. As a result, this means that the Commissioner responds directly to the interests and needs of the Minister which makes it difficult for them to be critical in their policy interventions. This stands in stark contrast with Competition Bureau Canada. Led by the Commissioner of Competition — who does not report directly to the Minister, but is appointed by the Governor in Council — is an "independent law enforcement agency that protects and promotes competition for the benefit of Canadian consumers and businesses."[11] The Commissioner of Competition is in charge of administering and enforcing the *Competition Act*, the *Consumer Packaging and Labelling Act*, the *Precious Metals Marking Act*, and the *Textile Labelling Act*.[12]

Furthermore, AIDA sets out provisions for the creation of an advisory committee — again at the discretion of the Minister. There are several problems with this:

1. Unclear and unaccountable convenings. The terms of reference for this committee have not been made available in the proposed law. As currently drafted, it seems as though the committee will meet only when the Minister wishes to discuss issues of interest to their office instead of matters of immediate public concern. The absence of details related to the committee's composition, report publication guidelines, chair and member term appointments, concentrate power in the hands of the Minister and obscure the regulatory process.

2. Limited capacity. The advisory committee is not an office staffed with personnel actively investigating issues. Additionally, the advisory committee is not provided with the financial resources nor the power to enforce AIDA itself. And although the experts may be enlisted in the committee, the technical expertise necessary to oversee the AI market in the Canadian context far exceeds the capacity that the committee may hold as they are not full-time employees.

3. Potential overlap with the existing Advisory Council. In 2019, the government launched the Government of Canada Advisory Council on Artificial Intelligence.[13] This Advisory Council was created to "ensure Canadians benefit from the growth of the AI sector" and "inform government policy in AI-related fields".[14]

4. Lack of enforcement power. Advisory committees are not enough to enforce and craft regulation. They are not meant to be the first reference points for regulatory oversight, and this is what we need.

Notable Examples of Robust Accountability through Independent Enforcement Bodies

There are numerous examples of regulatory bodies that the federal government could emulate for the enforcement of AIDA. For example, the European Commission's proposed regulatory framework for artificial intelligence includes the creation of a European Artificial Intelligence Board (EAIB). The Board will be composed of the European Data Protection Supervisor, the Commission, and national supervisory authorities. The role of the Board will be to facilitate the implementation of rules and regulations between the national supervisory authorities and the Commission itself.[15]

In the United States, the proposed Algorithmic Accountability Act of 2022 establishes the creation of the Bureau of Technology within the Federal Trade Commission (FTC). The FTC is an independent agency of the United States government, whose mandate is to enforce the American antitrust laws and promote consumer protection. The Bureau would be headed by a Chief Technologist and would require hiring a minimum of 50 new staffers within two years of the law's enactment. Moreover, the legislation would also require the appointment of 25 additional personnel to the enforcement division of the FTC's Bureau of Consumer Protection.[16] The proposed legislation sets that the bureau personnel should include people with "experience in fields such as management, technology, digital and product design, user experience, information security, civil rights, technology policy, privacy policy, humanities and social sciences, product management, software engineering, machine learning, statistics, or other related fields."[17]

What Should Adequate AI Oversight Look Like in Canada?

As it currently stands, AIDA provides the Minister with the ability to require that an audit be conducted if there are "reasonable grounds to believe" that contraventions to certain sections of the law have occurred.[18] The audit can be done internally by the company or by hiring the services of an independent auditor — at the expense and discretion of the company.[19] Furthermore, the proposed legislation requires companies to establish mitigating measures according to regulations — which have yet to be written — and also notify the Minister in the event that "the use of the system results or is likely to result in material harm", but only for systems that a provider deems to be "high-impact".[20]

As a result, oversight of algorithmic systems in this proposed legislation is primarily administered by the companies themselves in the form of audits. This is deeply concerning because research has demonstrated that the quality of audits is very poor when the auditee selects and compensates the auditor.[21] For example, a two-year study on environmental third-party audits found that audits were more accurate when auditors were not paid by the firm being audited, but instead by a common pool of government-distributed funding.[22] This is a trend that is unfortunately found in other areas, notably in credit rating agencies, supply chain and accounting audits.[23]

Moreover, allowing companies to choose their auditors opens the doors to conflicts of interests, cronyism and corruption. In the absence of regulations addressing auditor selection, there are no legally-binding provisions restricting companies from using firms that are led by family members, friends or other close personal relationships who could otherwise economically benefit from providing laxer audits.

As such, in order to improve the Canadian AI ecosystem, it is key that oversight be conducted independently from companies. This means that auditor selection, funding, and audit scope are not established by the audited company. Instead, audit practices should be determined by standards crafted by an independent regulatory tribunal or body. This entity would outline how audits ought to be conducted and how certification accreditation of auditors should be administered as well.

Independent oversight should extend beyond audits. Audits for algorithmic systems is not yet a professionally codified process, nor is it clear what

a professional approach should contain or even what discipline(s) should oversee it (e.g., computer science, engineering, statistics, actuarial science). Until such a time where there is a meaningful professional code, we believe that an multi-stakeholder independent oversight body should be empowered to contribute to the legislative process by developing or proposing laws and regulations, as well as enforcing legislation by having the ability to prohibit, restrict, withdraw and recall AI systems that do not comply with comprehensive legal requirements. This should include technical as well as non-technical expertise — and especially civil society representation.

Who Should be the Independent Oversight Body?

There are multiple pathways towards independent oversight. We outline below three potential avenues.

1. Office of the Privacy Commissioner of Canada (OPC)

Instead of its current ombudsperson role, the OPC could act as a regulator to verify compliance on demand — including when the OPC wishes to initiate an inquiry on its own due to the risks posed by an algorithmic system.[24] As the OPC argues in its annual report, these regulatory powers are frequent in Canada, notably in health and safety, food and restaurants, and in the tobacco industry.[25] For example, in the event of a salmonella outbreak in a given product, it is the role of the Canada Food Inspection Agency (CFIA) to conduct investigations, publish advisory notices and coordinate recalls.[26] Furthermore, the CFIA is responsible for the administration and enforcement of several acts such as the *Safe Food for Canadians Act*, the *Agriculture and Agri-Food Administrative Monetary Penalties Act*, and the *Fertilizers Act*.[27, 28]

An empowered OPC is not a novel idea, but rather in line with demands made by the OPC themselves and privacy scholars over the past few years.[29] In their 2016-2017 annual report, the OPC has stated that "the time has come for Canada to change its regulatory model [...] through privacy regulators who, like those of its trading partners in the U.S., the EU and elsewhere, have strong enforcement powers commensurate with the increasing risks that new disruptive technologies pose for privacy."[30] The OPC believes that such a "proactive enforcement model would be most effective in ensuring that organizations are demonstrably accountable for their protection of consumer privacy."[31]

2. Creation of an Independent Tribunal to administer and enforce AIDA

Bill C-27 includes the *An Act to establish the Personal Information and Data Protection Tribunal*, which creates an administrative tribunal that will hear appeals to decisions made by the OPC under the proposed CPPA. The tribunal is allowed to issue penalties for certain contraventions of the CPPA as well. A similar tribunal to administer and enforce AIDA would therefore be an interesting avenue for the government to follow. To be effective in its administration of AIDA, the independent regulatory body could be in charge of setting out standards for auditing practices, and enforcing the law's requirements by withdrawing and recalling AI products that are in contravention with AIDA.

3. Tribunal as set out in CCPA to include AIDA

However, seeing as issues related to privacy heavily overlap with artificial intelligence, an expanded tribunal that covers both the CCPA and AIDA would be an avenue that would avoid the duplication of these tasks.

Recommendations

- The AI and Data Commissioner is not an independent and powerful enough agent to administer AIDA. To effectively regulate the AI market in Canada, **the government needs to establish or empower an independent body that will be empowered to properly oversee and enforce AIDA.**

3. AIDA Must Apply to Government Institutions

In its current iteration, AIDA will only apply to the federal private sector. The law would not apply to all federal departments and Crown corporations nor to any system used by the Department of National Defence, Canadian Security Intelligence Service (CSIS), the Communications Security Establishment (CSE), or any other person who is responsible for federal or provincial departments or agencies and "who is prescribed by regulation".[32] This is a major problem given the known human rights risks of state-deployed AI systems as described in section 5 below — and as illustrated by the Royal Canadian Mounted Police's unlawful use of face recognition services provided by Clearview AI and the use of two AI-driven hiring services by the Department of National Defence.[33]

There is no legal or constitutional reason to exempt federal government institutions from AIDA, given their potential to pose serious harm to individuals through the use of AI or algorithmic systems. Such exemptions contradict AIDA's own stated purpose to "prohibit certain conduct" regarding AI systems that "may result in serious harm" to individuals.[34] The Directive on Automated Decision-Making that applies to certain federal government institutions' use of AI systems also contains numerous gaps[35] and fails to provide individuals with recourse, and is therefore not currently equipped to address the public safety and human rights risks related to the technology. Moreover, such government exemptions create problematic double-standards within Canadian AI regulation and further distance Canada from global accountability measures.[36]

Recommendations

- To properly address the public safety and human rights implications of AI systems, **AIDA needs to apply to all government institutions.**

4. Bill C-27 Needs Consistent, Technologically Neutral and Future-Proof Definitions

Bill C-27 proposes definitions of artificial intelligence that lack cohesion across the CPPA and AIDA. Any definition of AI within these laws ought to be technologically neutral and future-proof.

A Cohesive Definition of AI is Needed in the CPPA and AIDA

The CPPA and AIDA overlap but use different terms ("automated decision system" versus "artificial intelligence system") and define them differently, which ultimately leads to a lack of cohesion for one of the laws' central topics. Defining algorithmic or AI systems in different ways could lead to the uneven and unpredictable application of the two laws. For example, the CPPA captures only "automated decision systems" that "assist" or "replace" human judgment in decision-making contexts,[37] whereas AIDA refers to the "autonomous" or partially autonomous processing of data that generates content or "makes decisions, recommendations or predictions".[38] This is problematic given that the very same systems may be used in ways that infringe rights under the CCPA and AIDA. These different definitions of AI could very well mean that a person has recourse under only one of these laws due to the disparate and inconsistent definitions of AI across both laws.

There are concrete examples that highlight the problems that could arise due to the two different definitions of algorithmic systems currently found within the CPPA and AIDA. For example, if an "automated decision system" as defined by the CPPA is used for a decision where human judgment was never required before, then the CPPA would not capture this use of an algorithmic system.[39] Use of an algorithmic system that involves the processing of data related to *non-human* activities — such as activities related to institutions, technology, or other broader systems — would also mean that the CPPA could apply, but AIDA would not.[40] AIDA in its current state would also likely apply for the intentional generation of content or to make decisions, recommendations, or predictions, but the CPPA would apply only if an algorithmic system is used to assist or replace human decision-making. The list of techniques enumerated in each of the law's definitions is also different from each other, which would mean that an entity could attempt to avoid liability under one of the laws by attempting to claim that they did not use one of the techniques listed in one of the laws or that it did not use a technique that is similar to one that has been enumerated.

A cohesive definition of AI is also important across the CPPA and AIDA because these proposed laws balance the same interests. On the one hand, these laws balance the need for informational self-determination and the protection of human

Figure 1: The Different Definitions of AI or Algorithmic Systems Found Within Bill C-27

CPPA	AIDA
• "Automated decision system" • That assists or replaces the judgment of human decision-makers • Through the use of a rules-based system, regression analysis, predictive analytics, machine learning, deep learning, a neural network or other technique	• "Artificial intelligence system" • That autonomously or partially autonomously processes data related to human activities • Through the use of a genetic algorithm, a neural network, machine learning or another technique in order to generate content or make decisions, recommendations or predictions

rights related to the collection, use and disclosure of personal information when these actions are done with the assistance of algorithmic systems. On the other hand, the CPPA and AIDA also balance those interests with the desire of organizations to collect, make use of, and disclose personal information for their private interests. These two laws need to define AI or algorithmic systems in such a way that they regulate the same technology so that there is cohesion across both laws, both of which seek to hold organizations accountable for their use of the same technology in respect of privacy and human rights.

The Definition of AI or Algorithmic Systems Should Be Technologically Neutral, Future-Proof, and Address the Logic of these Systems

As the CPPA definition of "automated decision systems" and the AIDA definition of "artificial intelligence systems" stand, the proposed legislation could be circumvented by renaming, by disputes over categorization (e.g., statistics versus AI), or by unforeseen future developments (e.g., a new area using the same logic as AI but claiming to be a separate approach and branded differently).

Instead, we believe that the CPPA and AIDA both need a definition of AI that is technologically neutral and future-proof. By technologically neutral, we mean that the laws should address the source of concerns around a technology, rather than specific technologies. And by future-proof, we refer to how many of the issues around AI are not actually about AI itself, but underlying issues that the use of AI will exacerbate (e.g., sexism, racism, etc.). There will inevitably be future technological developments that fall outside of the label of "AI" but will raise the same concerns, and it is possible to have a definition that covers these.

In general, definitions of AI and machine learning (ML) from the field of computer science are frequently aspirational, describing what AI attempts to do (mimic human intelligence), rather than *how* it has succeeded in doing so. Similarly, outward-facing definitions of AI and ML again describe what these fields *seem* to be or seem to achieve, and not *how* they achieve those things.[i]

However, the concern regarding definitions should not be whether things are labeled as AI or ML, or if they employ one of the named techniques that are currently associated with AI or ML. Rather, both the CPPA and AIDA should address how decision-making rules learned from data can fail due to unrepresentative data, bad or manipulatable proxies, weak signals, and changes in context — to name a few examples.[41] Thus, to be future-proof, technologically neutral, and to address the core issues of concern, the federal government should consider working with technologists to define algorithmic systems based on their broad applications, instead of focusing on their techniques.

Both the CPPA and AIDA potentially fall short because their definitions focus on a limited number of techniques such as deep learning, predictive analytics, genetic algorithms, and machine learning. A potential pathway for legislation is to focus on how end-users interact with these technologies. As a result, both the CPPA and AIDA should cohesively define AI or algorithmic systems in ways that focus on, but are not limited to, their ability to generate outputs such as predictions, recommendations, and other types of decisions.

Recommendations

- The CCPA and AIDA should provide for a definition of AI or algorithmic systems that is **cohesive across both laws.**
- The definition of AI needs to be **technologically neutral** and **future-proof.**

i Exploration of the logic and fragilities underlining machine learning can be found in Appendix A. Appendix B examines how actuarial science uses machine learning approaches, which can help the federal government better understand how to define AI.

5. Bill C-27 Must Address the Human Rights Implications of Algorithmic Systems

The current draft of Bill C-27 fails to address the broad human rights implications of AI or algorithmic systems. The CPPA and AIDA need to ensure that the wide range of public safety and human rights issues engaged by the use of algorithmic systems are accounted for in a way that is precise yet comprehensive. The regulatory framework facilitated by AIDA should include provisions for prohibitions on unacceptable uses of algorithmic systems. Furthermore, this should translate into the adoption of obligations and rights needed when data is collected and processed through automated means particularly as it relates to vulnerable populations such as children.

Recordkeeping and Transparency Provisions Are Not Enough to Prevent Human Rights Violations

Obligations and rights in Bill C-27 that concern algorithmic systems focus primarily on recordkeeping and transparency, which does not prevent harms that may arise from their use. For example, section 62 of the CPPA requires organizations to make available to the public a general account regarding any use of any "automated decision system" that "could have a significant impact" on individuals.[42] Section 63(3) of the CPPA also provides individuals with the right to receive "an explanation" for any "prediction, recommendation or decision" that has a "significant impact" on them.[43] Similarly, requirements for organizations and people under AIDA are focused almost solely on keeping records, mitigating risks, and disclosing information related to those risks.[44] Moreover, AIDA addresses the impact and not the risk of systems, which as Scassa demonstrates, is problematic as the level of risk associated with the use of a system is not taken into account.[45]

There are prohibitions in AIDA that are useful first steps for addressing the privacy and human rights impacts of algorithmic systems. For example, the law prohibits the possession or use of personal information for the purpose of designing, developing, using, or making available for use an AI system if the information has been directly or indirectly obtained or derived from an illegal act in Canada.[46] AIDA also prohibits making an AI system available for use if the system (i) causes "serious physical or psychological harm to an individual or substantial damage to an individual's property" and if the person who made the system available did so "without lawful excuse and knowing that or being reckless" regarding this use, or (ii) causes "substantial economic loss to an individual" and if the person who made the system available did so "with intent to defraud the public and to cause substantial economic loss to an individual".[47]

However, under AIDA, there are a wide array of algorithmic systems — for example, face recognition technology for the unique identification of a person or AI systems used in the criminal justice system — that are not captured by these prohibitions. These systems may still be available for sale, provision, or use, despite the fact that such systems pose serious concerns from a human rights perspective.

Bill C-27 Fails to Address AI's Wide-Ranging Human Rights Implications

While AIDA addresses the possibility of various types of "harm", "biased output" and some limited prohibitions, there are numerous human rights risks related to algorithmic systems that go unaddressed in Bill C-27. From a privacy and human rights perspective, algorithmic systems may facilitate the violation of a wide range of rights at incredible speed and scale, and in ways that may be hidden or discreet as well as discriminatory and arbitrary.[48] As a result, it is not enough to legislate AI or algorithmic systems based on optimism of the technology's potential benefits or what it would hypothetically do in a perfect scenario. Instead, what is needed is an approach to the regulation of algorithmic systems

in Canada that both (i) identifies the technology's human rights risks and (ii) provides obligations and rights to properly address those critical risks.[49] In the following section, we discuss and provide examples of how human rights are implicated by algorithmic systems.

From a privacy perspective, algorithmic systems raise issues because constructing them requires the collection and processing of vast amounts of personal information, which can be highly invasive. The mere collection of this information can be privacy-intrusive particularly when it is done without consent, such as when information is scraped from the web or when information is used in a context that differs from the context in which the information was originally given.[50] Algorithmic systems can also be used to identify people where they may have the right to remain anonymous, and can be used to monitor people's political or sexual preferences, relationships, or travel patterns.[51] The re-identification of anonymized information, which can occur through the triangulation of data points collected or processed by algorithmic systems, is another prominent privacy risk.[52] The limited and weak requirements set out in the CPPA in tandem with the obligations of AIDA would appear to mean that it would be possible to lawfully collect, process, and disclose personal data simply because it is anonymized, which is not on its own enough to address the privacy risks related to the mass surveillance that is enabled by AI systems.[53]

From a broader human rights perspective, algorithmic systems can be used to facilitate violations of a wide range of rights on small and at times large scales. This is the case when the technology is used by entities that include but are not limited to law enforcement, public safety actors, judges, social service decision-makers, military actors, other third party service providers that are relied on by government actors, as well as online intermediaries such as social media platforms. There is a rich body of scholarly and interdisciplinary work that examines the human rights impacts of algorithmic systems, and, as such, this commentary will merely touch the surface on this topic.[54]

The following is a non-exhaustive overview of the human rights risks related to the use of AI systems. These risks are not adequately addressed within AIDA nor in the CPPA.

Figure 2: A Non-exhaustive Overview of the Human Rights Implicated by AI or Algorithmic Systems

Application of AI Systems	Implicated Human Rights	Explanation
Content moderation by online service providers	Data protection and privacy rights Freedom of expression and association Equality rights or freedom from discrimination	Online service providers such as social media platforms and other intermediaries can use AI systems for the automated filtering and blocking of content.[55] The collection of personal data required to filter content raises privacy and data protection issues. The blocking of content implicates free expression rights. The uneven or discriminatory filtering and blocking of content could also result in the violation of equality rights.
The prediction and prevention of wrongdoing and illegal activity by law enforcement and public safety actors	Data protection and privacy rights Freedom of expression and association Equality rights or freedom from discrimination The right to life, liberty, and security of the person Freedom from unreasonable search and seizure Freedom from arbitrary detention or imprisonment	Law enforcement and public safety actors can use AI systems to detect, predict, and/or prevent wrongdoing or criminal activity, with tools available such as such as gunshot detection, image recognition for photos and videos, and crime hotspot prediction. AI systems can enable the rapid collection of mass amounts of information in the public safety context, which can increase the speed with which people are detained and arrested. In turn, arbitrary and discriminatory decisions may occur more quickly and at higher rates than when the technology is not used. Researchers at Citizen Lab have highlighted the wide range of human rights risks posed by such technology, and researchers at Toronto Metropolitan University have also identified the particular risks related to the use of face recognition technology.[56]
Rendering decisions by courts, tribunals, and other government actors	Procedural fairness The right to an impartial decision-maker Equality rights or freedom from discrimination The right to life, liberty, and security of the person	The use of algorithmic systems by certain legal decision-makers may implicate certain rights such as the right to an impartial decision-maker and freedom from bias, such as when the technology is used for decisions related to immigration or receiving social services or welfare.[57] The right to life, liberty, and security of the person may also be implicated when AI is used to facilitate a person's deportation. Additionally, the use of AI in the criminal justice system particularly raises issues regarding the right to procedural fairness and the right to freedom from discrimination, including but not limited to when the technology is used for bail and sentencing decisions.[58]
In military or war-time contexts	The right not to be subject to torture or to cruel, inhuman, or degrading treatment or punishment For those who are outside of combat and those not taking part in hostilities where there is armed conflict, the right to be protected in all circumstances The right to freedom from unfair detainment	When algorithmic systems are used in military or war-time contexts — including systems such as facial recognition technology, drones, robots, and lethal autonomous weapons — then a wide range of international human rights and humanitarian laws could come into play when the technology is used to facilitate arbitrary arrests and detention, deportation, torture, and other grave human rights abuses.[59] Civil society organizations in the EU have called on lawmakers to set clear safeguards for such systems that are used for military and national security purposes.[60]

Certain Uses of Algorithmic Systems Are Unacceptable and Must Be Prohibited

The current approach to addressing risk within AIDA is currently ill-equipped to respond to the wide range of human rights risks posed by algorithmic systems.[61] Allowing the use of certain algorithmic systems and in certain contexts may also pose such significant risks to people's safety, livelihoods, and rights that such uses cannot be allowed in a free and democratic society. In the following section, we discuss examples of algorithmic system applications that should be prohibited or at the very least accounted for within AIDA and within the CPPA where needed.

AI Systems that Impact the Health and Financial Outcomes for Individuals and Communities

There is a rich body of scholarly and policy works on the human rights impacts of algorithmic systems, such as the possibility for the use of the technology to affect people's well-being and financial situations.[62] In these contexts, algorithmic systems may not be used in such a way where rights are outright violated. Instead, there are deleterious impacts or risks stemming from use of the technology concerning people's financial situations or physical and/or psychological well-being. The primary issue here is that a significant amount and type of personal information can be gathered that is used to surveil and "socially sort" or profile individuals and communities, as well as forecast and influence their behaviour.[63]

We urge Canadian policymakers to consult and adequately address these issues in Bill C-27 prior to its potential enactment. In comparison to laws that exist or are emerging in the EU, the processing of health data is of such concern that the GDPR prohibits the automated processing, including profiling, based on this type of data with certain exceptions and only if suitable measures are in place that safeguard rights and freedoms as well as legitimate interests.[64] The draft EU AI Act also prohibits the use of algorithmic systems by public authorities, or on their behalf, for social scoring purposes and if the score leads to (a) detrimental or unfavourable treatment of people in social contexts that are unrelated to the contexts in which the data was originally generated or collected and/or (b) detrimental or unfavourable treatment of people that is unjustified or disproportionate to the social behaviour or its gravity.[65] By failing to address the ability for algorithmic systems to detrimentally impact people's health and financial outcomes, the CPPA and AIDA are both falling far behind data protection and human rights standards.[66]

The Use of Biometric or Health-Related Bodily Information for AI Systems

The collection and processing of biometric information (such as facial images) for the purposes of uniquely identifying people through automated means for public safety purposes poses significant concerns from a human rights perspective. Both politicians as well as civil society organizations around the globe are calling for a prohibition on the use of such biometric recognition practices given the related myriad human rights risks.[67]

Experts note that the use of algorithmic systems to analyze and categorize people on the basis of their biometric and other health-related bodily information can be seen as an extension of physiognomy, or a debunked and type of discredited junk science that examines biological and facial features with a view to ascertain one's propensity for certain (including criminal) behaviour.[68] The use of biometric recognition and categorization systems can further facilitate systemic discrimination and historical inequities related to various bases of discrimination — what Stark and Hutson have aptly referred to as the use of technology to "infer or create hierarchies of an individual's body composition, protected class status, perceived character, capabilities, and future social outcomes based on their physical or behavioral characteristics".[69]

In contrast to aIDA, the proposed EU AI Act would prohibit the use of real-time remote biometric identification systems in publicly accessible spaces for law enforcement purposes except in specific circumstances, and a wide range of civil society organizations in the EU are urging policymakers

there to require a blanket prohibition on the use of remote biometric identification in any circumstances and by all actors.[70] Other civil society actors are also calling for a prohibition on the use of remote biometric recognition systems in publicly accessible spaces for the purposes of categorizing people (based on those biometric characteristics) given the risks of discriminatory impacts.[71]

The need for a prohibition on the use of facial recognition technology for the unique identification of individuals by public safety actors in Canada is a message that we have also repeatedly urged policymakers to take note of and establish within Canadian law.[72]

The Use of AI Systems for Access to Social Services or Humanitarian Aid

Algorithmic systems can also be used in public sector contexts to assess a person's ability to receive social services such as welfare or humanitarian aid, which can result in discriminatory impacts on the basis of socio-economic status, geographic location, amongst other data points analyzed.[73]

As raised earlier, recall that the proposed EU AI Act would prohibit the use of algorithmic systems by public authorities (or on their behalf) for social scoring purposes and if the score leads to (a) detrimental or unfavourable treatment of people in social contexts that are unrelated to the contexts in which the data was originally generated or collected and/or (b) detrimental or unfavourable treatment of people that is unjustified or disproportionate to the social behaviour or its gravity.[74]

Canada is falling behind this emerging legal standard set out in the EU AI Act. Instead, the collection and use of sensitive biometric data for analysis through algorithmic systems and for life-altering, health- and financial-related recommendations or decisions remains inadequately addressed within the CPPA and AIDA, which is a major oversight in Bill C-27 as a whole.

AI Systems That Profile People and Influence Their Behaviour

Algorithmic systems can also be used to profile and influence people's behaviour, with particularly deleterious impacts on vulnerable populations such as children or disabled people. The primary issue here also concerns the use of algorithmic systems to surveil and profile people, often with a view to forecast or influence their behaviour. For example, consider the case of Facebook-Cambridge Analytica data scandal, where the public learned in 2018 that Cambridge Analytica had harvested the personal data of up to 87 million Facebook users for analysis and profiling through machine learning — for the purpose of providing targeted political ads to those voters in hopes of swaying their vote in various elections.[75]

However, such data mining and targeted messaging can cause or enable harm to vulnerable groups, such as those who lack legal capacity such as children and disabled people. For instance, algorithmic systems for recommending content on websites and social media platforms to children based on their activity, despite the risks of them being shown content that may be inappropriate for them from a child development perspective or that may serve to radicalize them politically.[76] Companies such as Facebook (now Meta) have also allowed teens as young as 13 to be targeted with ads for alcohol, drugs and extreme weight loss.[77] Even more troubling than this is the fact that recent internal Facebook documents reveal the company was aware of how their products and services harm children and youth, further underscoring the need for robust accountability and oversight measures.[78]

These outcomes are of such significant concerns from a human rights perspective that the proposed EU AI Act would prohibit "practices that have a significant potential to manipulate persons through subliminal techniques beyond their consciousness or exploit vulnerabilities of specific vulnerable groups such as children or persons with disabilities in order to materially distort their behaviour in a manner that is likely to cause them or another person psychological or physical harm."[79] The EU AI Act also provides a specific prohibition on such practices when they are used to exploit vulnerable groups based on their age or physical and mental disability.[80] These risks go unaddressed in Bill C-27, which is a major oversight that must be rectified for future versions of the CPPA and AIDA to properly account for the human rights risks related to algorithmic systems.

Children and Young People's Rights Related to AI Systems Need to be Addressed

The stakes of neglecting to mitigate risks to children and young people before they materialize into harm are significant, particularly given children's developmental vulnerabilities and their status as 'early adopters' of emerging technologies. In fact, these very characteristics afford children special considerations in internationally recognized human rights law, including the *United Nations Convention on the Rights of the Child (UNCRC)*, of which Canada is a signatory. Without affording children's rights extra protections, AIDA risks flattening the impact from known privacy risks across groups that are differentially and disproportionately affected by AI systems.

Canadian and international organizations alike have emphasized the need to incorporate proactive measures such as clear instructions for the *design* and *testing* of AI products and services before they are deployed (or modified).[81] This is reflected by growing policy trends to embed robust children's rights impact assessments, auditing measures and accountability mechanisms into legislative efforts around the world. Such systemic approaches are already seeing success in California, the European Union, and notably, the UK, which recently passed the *Age Appropriate Design code* which mandates how children's data are collected, used, and sold by setting high levels of data privacy and protections for children under 18. The Code also sets out specific design obligations for developers of services "likely to be accessed by children" by requiring that the best interest of the child be a primary consideration during design and development.[82]

The federal government ought to learn from these emerging best practices related to children's rights that are implicated when AI systems are used, and children should be given special category status and protection within Bill C-27 and in AIDA more specifically.

Recommendations

- **The CCPA and AIDA need to address the human rights risks of algorithmic systems in a comprehensive manner.** Bill C-27 and AIDA need amendments to protect fundamental rights when AI systems are used — such as the right to object to the automated processing of personal data, as well as the right to appeal decisions that are made when algorithmic systems are used.
- In line with our previous findings on the topic and with relevant global human rights efforts, **Bill C-27 needs to have a framework addressing the collection and processing of biometric data.** This framework should include, but not be limited to, prohibitions on the processing of biometric data such as facial images through automated means for the unique identification of individuals, especially in public settings and potentially subject to a very limited set of exceptions.
- **Certain other uses of algorithmic systems must also not be allowed because they pose unacceptable risks to people's safety, livelihoods, and rights, which requires more than AIDA's current two-tiered system.** These prohibitions should include but are not limited to the use of algorithmic systems that exploit vulnerable groups based on their age (such as children) or physical and mental disabilities, as well as systems that are used by public authorities for social scoring purposes that lead to detrimental or unfavourable treatment that is unjustified. The drafters of Bill C-27 need to collaborate with and draw on the work of human rights experts and experts on algorithmic systems to properly craft the changes needed to the proposed laws.
- Bill C-27 and AIDA more specifically should include **special category status for children (under 18)** given international human rights law precedent, and should require high levels of protection by default, especially against commercial use of children's data.

Appendix A

Machine learning models are built on statistical techniques, but in contrast to how traditional statistical modeling has been used to try and understand the world, machine learning models search only for optimal correlations.[83] A *correlation*, in statistics and machine learning, is when some attributes (like height and weight), measured over multiple entities (the height and weight of multiple people), have values that tend to vary in the same ways (taller people tend to be heavier, and vice versa). A *model* is a way to measure correlations between sets of attributes and then use those measured correlations to try to anticipate the value of some target attribute (e.g., using past purchasing behaviour to anticipate future purchasing behaviour).

Machine learning has developed powerful ways of automatically finding correlations, for example deep learning models ("deep" refers to the model having many layers, and *not* to the model being profound) can find correlations between *groupings of pixels* and human-given labels for images, which drives automatic image labeling and the ability to recognize specific people in pictures.

However, the caveat that "correlation is not causation" applies: while machine learning can find correlations, it cannot determine whether these are causal or not, which makes machine learning models potentially very fragile. For example, the way deep learning models find patterns of pixels does *not* correspond to humans visual processing, meaning that deep learning models for image recognition can be fooled by manipulating images in ways that are not noticeable to human viewers.[84, 85] Short of experimentation such as randomized control trials, statistics too cannot reliably identify causation either; but traditionally, statistics has attempted to use theoretical reasoning to identify what correlations might be causal, yet this reasoning is usually absent in machine learning.

Appendix B

Note that finding optimal correlations is not unique to machine learning; *actuarial science*, which uses statistical models for making credit and insurance decisions and for making criminal justice decisions (bond, sentencing, parole) related to potential recidivism,[86] have been employing the same logic long before machine learning[87] (sometimes even developing techniques in parallel with machine learning[88]).

Horror stories of actuarial science, or even how rates can seem arbitrary (because correlations are not always obvious from the perspective of an individual) or unfair[89] (because a correlation can come from injustice, not something within people's control), and how people are often effectively punished or rewarded for things outside of their control (which, at its worst, is effectively "pil[ing] on" further punishment to those who are already "victims of injustice and cruelty"[90]), are a direct precedent for horror stories of AI.

This is not to say that existing regulation for these practices could be a model for regulating AI, because there are strong arguments about how those regulations are systematically insufficient.[91] For example, not using race as an explicit input for credit decisions and insurance rates may not *formally* (directly) perpetuate racial bias, but it does so *substantively* (indirectly): legacies of redlining and segregation make postal code an effective proxy for both race, and for living in communities suffering from systematic deprivation that tends to make individuals more frequently have bad insurance-related outcomes. Allowing the approach of individualizing risk based on correlates thus results in additional insurance burdens on communities of color;[92] bans on the use of race in credit decisions and insurance rates are insufficient for preventing *substantive* discrimination on the basis of race.

This also shows that AIDA's reference to "biased output" is subjective: is output biased if it substantively perpetuates inequality, or — if it "merely" empirically, and accurately, reflects the status quo of a biased society — should it be considered unbiased? If we recognize that we need to make normative, moral decisions about what in the empirical status quo should count as "biased" and by how much, who makes these decisions?[93]

Regulation needs to consider when it is appropriate and morally justified to characterize "risk" (as an abstraction of negative outcomes) purely empirically in order to *individualize* it[94] for formal equality, or when the pursuit of equity and justice through substantive equality demand that risk (or other targets of machine learning) should instead be *collectivized*[95] such as in nationalized insurance systems, of the type that exist in Canada for health insurance (but not for loans, or for car or life insurance).

References

[1] Views expressed in this submission are independent views of the authors and do not reflect those of their partnering institutions. This commentary was drafted before the completion of the Report of the Standing Committee on Access to Information, Privacy and Ethics (ETHI), Facial Recognition Technology and the Growing Power of Artificial Intelligence, released in October 2022.

[2] Scassa, Teresa. "Oversight and Enforcement Under Canada's Proposed AI and Data Act." Web log, August 29, 2022. 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.

[3] Hayes, Helen A. "Roundtable on the Artificial Intelligence and Data Act." Centre for Media, Technology and Democracy. Accessed September 12, 2022. https://www.mediatechdemocracy.com/events/roundtable-on-the-artificial-intelligence-and-data-act.

[4] "Consultation Documents." Investment Canada Act. Innovation, Science and Economic Development Canada, February 15, 2022. , Canada. Innovation, Science, Economic Development Canada. *National Quantum Strategy Consultations: What We Heard Report*, July 18, 2022. https://ised-isde.canada.ca/site/national-quantum-strategy/en/national-quantum-strategy-consultations-what-we-heard-report#s1.2 https://www.ic.gc.ca/eic/site/ica-lic.nsf/eng/h_lk00074.html.

[5] "Public Consultations." Office of the Superintendent of Bankruptcy Canada. Innovation, Science and Economic Development Canada, August 26, 2019. https://www.ic.gc.ca/eic/site/bsf-osb.nsf/eng/h_br02431.html.

[6] The *Consumer Privacy Protection Act* (CPPA) and the *Artificial Intelligence and Data Act* (AIDA) in 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*, 1 sess., 44th Parliament, 2022. Section 2(1) of the CPPA and section 5(1) of AIDA currently define Minister as "the member of the Queen's Privy Council for Canada designated [...] or, if no member is so designated, the Minister of Industry."

[7] Ifill, Erica. "Liberals on Collision Course to Entrench Anti-Blackness." Not In My Colour, June 22, 2022. https://notinmycolour.com/liberals-on-collision-course-to-entrench-anti-blackness/

[8] Witzel, Mardi. "A Few Questions about Canada's Artificial Intelligence and Data Act." Centre for International Governance Innovation, August 11, 2022. https://www.cigionline.org/articles/a-few-questions-about-canadas-artificial-intelligence-and-data-act/.

[9] Ifill, Erica. "Liberals on Collision Course".

[10] AIDA, s. 33-35.

[11] "Competition Bureau Canada." Government of Canada, September 22, 2022. https://www.competitionbureau.gc.ca/eic/site/cb-bc.nsf/eng/home.

[12] "Our Mandate." Competition Bureau Canada, January 20, 2022. https://www.competitionbureau.gc.ca/eic/site/cb-bc.nsf/eng/00020.html.

[13] "Terms of Reference of the Government of Canada Advisory Council on Artificial Intelligence" Innovation, Science and Economic Development Canada, January 28, 2022. https://ised-isde.canada.ca/site/advisory-council-artificial-intelligence/en/terms-reference-government-canada-advisory-council-artificial-intelligence, s. 4(d).

[14] "Terms of Reference of the Government of Canada Advisory Council on Artificial Intelligence" Innovation, Science and Economic Development Canada, January 28, 2022. https://ised-isde.canada.ca/site/advisory-council-artificial-intelligence/en/terms-reference-government-canada-advisory-council-artificial-intelligence, s. 4(d).

[15] Madiega, Tambiama. "Artificial Intelligence Act ." European Parliamentary Research Service, January 2022. https://www.europarl.europa.eu/RegData/etudes/BRIE/2021/698792/EPRS_BRI(2021)698792_EN.pdf. p. 7.

[16] Algorithmic Accountability Act of 2022, H.R. 6580, 117th Cong. s.8(4) https://www.congress.gov/117/bills/hr6580/BILLS-117hr6580ih.pdf.

[17] Algorithmic Accountability Act of 2022, s. 8(3).

[18] AIDA, s. 15.

[19] AIDA, s. 15.

[20] AIDA, s. 9 and s. 12.

[21] Raji, Inioluwa et al. "Outsider Oversight": Designing a Third Party Audit Ecosystem for AI Governance." In *Proceedings of the 2022 AAAI/ACM Conference on AI, Ethics, and Society*, 557–71. Oxford United Kingdom: ACM, 2022. https://doi.org/10.1145/3514094.3534181, p. 9.

[22] Duflo, Esther et al. "Truth-Telling by Third-Party Auditors and the Response of Polluting Firms: Experimental Evidence from India." *The Quarterly Journal of Economics* 128, no. 4 (November 1, 2013): 1499–1545. in Raji et al. "Outsider Oversight".

[23] Raji et al. "Outsider Oversight", p. 9.

[24] For more on the need to strengthen the enforcement powers of the OPC, see: Scassa, Teresa, "Moving on From the Ombuds Model for Data Protection in Canada", *Canadian Journal of Law and Technology* 17, no. 1 (2019), https://digitalcommons.schulichlaw.dal.ca/cjlt/vol17/iss1/5/.

[25] Office of the Privacy Commissioner of Canada. "Annual Report to Parliament on the Personal Information Protection and Electronic Documents Act and the Privacy Act", 2017. https://www.priv.gc.ca/media/4586/opc-ar-2016-2017_eng-final.pdf, p. 33.

[26] Canadian Food Inspection Agency. "How We Decide to Recall a Food Product." Canadian Food Inspection Agency. Government of Canada, August 9, 2022. https://inspection.canada.ca/food-safety-for-consumers/canada-s-food-safety-system/how-we-decide-to-recall-a-food-product/eng/1332206599275/1332207914673.

[27] *Canadian Food Inspection Agency Act*, s. 11(1).

[28] "Most recalls in Canada are voluntary, meaning that they are conducted by the responsible company with oversight from the CFIA. If a company is unable or refuses to conduct a voluntary food recall, the Minister of Health has the power to order a mandatory recall for all food that poses a health risk." as outlined in "How We Decide to Recall" https://inspection.canada.ca/food-safety-for-consumers/canada-s-food-safety-system/how-we-decide-to-recall-a-food-product/eng/1332206599275/1332207914673. Additionally, the Canadian Food Inspection Agency Act in s. 19 grants the Minister of Agriculture and Agri-Food the power to conduct a mandatory recall as well.

[29] Cofone, Ignacio. "Policy Proposals for PIPEDA Reform to Address Artificial Intelligence Report." Office of the Privacy Commissioner of Canada, November 12, 2020. https://www.priv.gc.ca/en/about-the-opc/what-we-do/consultations/completed-consultations/consultation-ai/pol-ai_202011.

[30] "Annual Report to Parliament on PIPEDA", 2017 p. 31.

[31] "Annual Report to Parliament on PIPEDA", 2017, p. 33 .

[32] AIDA, s. 3.

[33] Office of the Privacy Commissioner of Canada, "Joint investigation of Clearview AI, Inc. by the Office of the Privacy Commissioner of Canada, the Commission d'accès à l'information du Québec, the Information and Privacy Commissioner for British Columbia, and the Information Privacy Commissioner of Alberta" (2 February 2021), www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-businesses/2021/pipeda-2021-001/; Cardoso, Tom and Bill Curry. "National Defence skirted federal rules in using artificial intelligence, privacy commissioner says," *The Globe and Mail*, February 7, 2021. https://www.theglobeandmail.com/canada/article-national-defence-skirted-federal-rules-in-using-artificial/.

[34] AIDA, s. 4.

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

[36] Hayes, Helen. "Centre for Media, Technology and Democracy Roundtable on the Artificial Intelligence and Data Act." July 7, 2022. https://www.mediatechdemocracy.com/events/roundtable-on-the-artificial-intelligence-and-data-act; see also European Parliamentary Research Service. "Regulatory divergences in the draft AI act: Differences in public and private sector obligations." *Panel for the Future of Science and Technology*. 2022. https://www.europarl.europa.eu/RegData/etudes/STUD/2022/729507/EPRS_STU(2022)729507_EN.pdf, which found that there is a convergence of risks regarding the use of AI in both the public and private sectors.

[37] CPPA, s. 2(1).

[38] AIDA, s. 2.

[39] Jonathan Mayer (Assistant Professor at Princeton University), in discussion with the authors, August 2022.

[40] Jonathan Mayer (Assistant Professor at Princeton University), in discussion with the authors, August 2022.

[41] Sayash Kapoor (Graduate student at Princeton University), in discussion with the authors, October 2022.

[42] CPPA, s. 62.

[43] CPPA, s. 63. On top of this, the CPPA fails to define what "significant impact" means.

[44] For example, sections 6 to 12 of AIDA impose requirements related to the anonymization of data; assessment of whether a system is "high impact"; mitigating the "risks of harm" or "biased output"; keeping general records regarding anonymization and risk mitigation efforts; explanations for the public on how systems will be used, outputs, and risk mitigation efforts; and, as mentioned earlier in section 2, notification to the Minister if the use of a system results or is likely to result in "material harm". The Minister can prohibit the sale, provision, or use of an algorithmic system, but only if the Minister has reasonable grounds to believe that the system "gives rise to serious risk of imminent harm." However, the Minister can only make this order for systems that have been deemed by system providers as "high-impact" — which may disincentivize the categorization of systems as "high-impact" in the first place.

[45] Scassa, Teresa. "Canada's Proposed AI & Data Act - Purpose and Application."

[46] AIDA, s. 38.

[47] AIDA, s. 39.

[48] See e.g., Stevens, Yuan, Ana Qarri, Sam Andrey, and Joe Masoodi. "Face Recognition Technology for the Protection of Canada's Parliamentary Precinct and Parliament Hill? Potential Risks and Considerations." Policy report, April 2022. https://www.ryersonleadlab.com/frt-parliament-hill.

[49] See e.g., Raji, Inioluwa Deborah, I. Elizabeth Kumar, Aaron Horowitz, and Andrew D. Selbst. "The Fallacy of AI Functionality," In *2022 ACM Conference on Fairness, Accountability, and Transparency*, 1-22. Seoul, Republic of Korea: ACM, 2022. https://doi.org/10.1145/3531146.3533158.

[50] This point was raised well in landmark work done by Tamir Israel: "Facial Recognition at a Crossroads: Transformation at our Borders and Beyond," Samuelson-Glushko Canadian Internet Policy & Public Interest Clinic (CIPPIC), 2020. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3714297.

[51] Stevens, Yuan, Ana Qarri, Sam Andrey, and Joe Masoodi. "Face Recognition Technology for the Protection of Canada's Parliamentary Precinct and Parliament Hill? Potential Risks and Considerations."

[52] It is clear that the drafters of AIDA see anonymized data as one of the primary ways to facilitate the protection of privacy. S. 6 of AIDA states that anyone who engages in "regulated activity" and who "processes or makes available for use anonymized data" in the course of that activity has to follow the rules in the regulations re: (a) how that data is anonymized and (b) the use or management of this data. However, these requirements are left out of the law and put into the regulations. More than this, research demonstrates that "heavily" incomplete and anonymized datasets can still result in the re-identification of individuals; in a 2019 study, researchers found that they were able to re-identify 99.98% of people in a given sample using 15 demographic attributes in an otherwise anonymized dataset, which challenges the assumption that the de-identification of data is sufficient to protect privacy: Rocher, Luc Julien M. Hendrickx, and Yves-Alexandre de Montjoye. "Estimating the success of re-identifications in incomplete datasets using generative models," *Nature Communications* 10, no. 3069 (2019). https://www.nature.com/articles/s41467-019-10933-3/.

[53] Office of the Privacy Commissioner of Canada, "Joint investigation of Clearview AI, Inc."

[54] See e.g., Abdurahman, J. Khadijah, "Birthing Predictions of Premature Death," *LOGIC*, August 2022, https://logicmag.io/home/birthing-predictions-of-premature-death/. Benjamin, Ruha. *Race After Technology: Abolitionist Tools for the New Jim Code*. (Polity, 2019), https://www.ruhabenjamin.com/race-after-technology; Eubanks, Virginia. *Automating Inequality: How High-Tech Tools Profile, Police, and Punish the Poor*. (St. Martin's Press, 2018), https://us.macmillan.com/books/9781250074317/automatinginequality; Chun, Wendy Hui Kyong. *Discriminating Data: Correlation, Neighborhoods, and the New Politics of Recognition*. (The MIT Press, 2021), https://mitpress.mit.edu/9780262046220/discriminating-data/; Robertson, Kate, Cynthia Khoo, and Yolanda Song. 2020. "To Surveil and Predict: A Human Rights Analysis of Algorithmic Policing in Canada." Policy report, Citizen Lab at the Munk School of Global Affairs & Public Policy and the University of Toronto's International Human Rights Program (IHRP) at the Faculty of Law, September 1, https://citizenlab.ca/2020/09/to-surveil-and-predict-a-human-rights-analysis-of-algorithmic-policing-in-canada/.

[55] See e.g., Stevens, Yuan and Vivek Krishnamurthy. *Overhauling the Online Harms Proposal in Canada: A Human Rights Approach*, https://cippic.ca/sites/default/files/Online%20Harms%20Submission%20Final%202021-09-27.pdf; Tenove, Chris, Heidi Tworek, and Fenwick McKelvey. 2018. "Poisoning democracy: how Canada can address harmful speech online." White paper. Public Policy Forum. November 8. https://ppforum.ca/publications/poisoning-democracy-what-can-be-done-about-harmful-speech-online/; Llansó, Emma, Joris Van Hoboken, Paddy Leerssen, and Jaron Harambam. 2020. "Artificial Intelligence, Content Moderation, and Freedom of Expression." White paper. Transatlantic Working Group on Content Moderation Online and Freedom of Expression, February 26. https://www.ivir.nl/publicaties/download/AI-Llanso-Van-Hoboken-Feb-2020.pdf.

[56] See e.g., Robertson, Kate, Cynthia Khoo, and Yolanda Song. "To Surveil and Predict: A Human Rights Analysis of Algorithmic Policing in Canada"; Stevens, Yuan, Ana Qarri, Sam Andrey, and Joe Masoodi. *Face Recognition Technology for the Protection of Canada's Parliamentary Precinct and Parliament Hill? Potential Risks and Considerations*.

[57] See e.g., Molnar, Petra and Lex Gill. 2018. "Bots at the Gate: A Human Rights Analysis of Automated Decision-Making in Canada's Immigration and Refugee System." Report, University of Toronto's International Human Rights Program (IHRP) at the Faculty of Law and the Citizen Lab at the Munk School of Global Affairs and Public Policy, https://citizenlab.ca/2018/09/bots-at-the-gate-human-rights-analysis-automated-decision-making-in-canadas-immigration-refugee-system/; James, Alexandra and Andrew Whelan. "'Ethical' artificial intelligence in the welfare state: Discourse and discrepancy in Australian social services." *Critical Social Policy* 42, no. 1 (2021): 22-42. https://journals.sagepub.com/doi/abs/10.1177/0261018320985463; Langford, Malcolm. "Taming the Digital Leviathan: Automated Decision-Making and International Human Rights." *AJIL Unbound* 114 (2020): 141-46. https://www.cambridge.org/core/journals/american-journal-of-international-law/article/taming-the-digital-leviathan-automated-decisionmaking-and-international-human-rights/5AFE96F03A1B75B63729D60F0F609609.

[58] See e.g., Brenner, Michael, Jeannie Suk Gersen, Michael Haley, Matthew Lin, Amil Merchant, Richard Jagdishwar Millett, Suproteem K. Sarkar, Drew Wegner. "Constitutional Dimensions of Predictive Algorithms in Criminal Justice." *Harvard Civil Rights - Civil Liberties Law Review* 55 (2020): 267-310. https://heinonline.org/HOL/LandingPage?handle=hein.journals/hcrcl55&div=9&id=&page=; Okidegbe, Ngozi. "The Democratizing Potential of Algorithms?." *Connecticut Law Review, Forthcoming 2021, Cardozo Legal Studies Research Paper* 655 (2020). https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3835370.

[59] See e.g., UNHR. "International Legal Protection of Human Rights in Armed Conflict." 2011. https://www.ohchr.org/sites/default/files/Documents/Publications/HR_in_armed_conflict.pdf.

[60] European Center for Not-for-Profit Law. "Scope of the EU Artificial Intelligence Act (AIA): Military Purposes and National Security." *Artificial Intelligence Act Amendments*. 2022. https://ecnl.org/news/eu-ai-act-needs-clear-safeguards-ai-systems-military-and-national-security-purposes.

[61] Ss. 29-30 of AIDA discuss types of violations as "minor", "serious", or "very serious", but the definition of these categories of violations is yet again undefined in the body of the law, leaving the public with little ability to understand how and to trust that the human rights risks of AI systems will be adequately addressed by the law as a whole.

[62] For further analysis of AIDA's problems regarding its somewhat obsessive focus on the individual rather than communities, see work by Teresa Scassa: "The unduly narrow scope for 'harm' and 'biased output' under the AIDA." Web log, August 22, 2021. 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.

[63] See e.g., Lyon, David. *Surveillance as social sorting*. (London: Routledge, 2002). https://www.taylorfrancis.com/chapters/edit/10.4324/9780203994887-6/surveillance-social-sorting-david-lyon; European Parliamentary Research Service. "The impact of the General Data Protection Regulation (GDPR) on artificial intelligence." *Panel for the Future of Science and Technology*. 2020. https://www.europarl.europa.eu/RegData/etudes/STUD/2020/641530/EPRS_STU(2020)641530_EN.pdf at s. 2.3.4.

[64] 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) (Text with EEA relevance), OJ L 119, 4.5.2016, p. 1–88 (GDPR), Article 22(4). The EU AI Act also categorizes algorithmic systems as "high-risk" if they fall under pre-existing EU health and safety harmonization. See Madiega, Tambiama. "Artificial intelligence act." European Parliamentary Research Service. January 2022. https://www.europarl.europa.eu/RegData/etudes/BRIE/2021/698792/EPRS_BRI(2021)698792_EN.pdf at page 5.

[65] Proposal for a Regulation of the European Parliament and of the Council Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts COM/2021/206, (EU AI Act), article 5(1)(c).

[66] There are other human rights implications of AI systems that should be addressed within the law, including but not limited to the use of AI for immigration decisions. Molnar, Petra and Lex Gill. 2018. "Bots at the Gate: A Human Rights Analysis of Automated Decision-Making in Canada's Immigration and Refugee System."

[67] See e.g., Lomas, Natasha. "European Parliament backs ban on remote biometric surveillance," Tech Crunch, October 6, 2021. https://techcrunch.com/2021/10/06/european-parliament-backs-ban-on-remote-biometric-surveillance/; and Stevens, Yuan, Ana Qarri, Sam Andrey, and Joe Masoodi. "Face Recognition Technology for the Protection of Canada's Parliamentary Precinct and Parliament Hill? Potential Risks and Considerations", which cites Amnesty International. "Inside the NYPD's Surveillance Machine." https://banthescan.amnesty.org/; Reclaim Your Face. "About the movement." https://reclaimyourface.eu/the-movement/; Ban Facial Recognition. "Ban Facial Recognition." https://www.banfacialrecognition.com/.; International Civil Liberties Monitoring Group. "Open Letter: Canadian Government must ban use of facial recognition by federal law enforcement, intelligence agencies." https://iclmg.ca/facial-recognition-letter/. See also, Daigle, Thomas. "Clearview AI facial recognition offers to delete some faces - but not in Canada," CBC, June 10, 2020. https://www.cbc.ca/news/science/clearview-ai-canadian-data-1.5605258.

[68] Todorov, Alexander. "Can we read a person's character from facial images?." Scientific American, May 14, 2018. https://blogs.scientificamerican.com/observations/can-we-read-a-persons-character-from-facial-images/.

[69] Stark, Luke and Jevan Hutson. "Physiognomic Artificial Intelligence." *Fordham Intellectual Property, Media & Entertainment Law Journal* 32 (2022). https://ir.lawnet.fordham.edu/iplj/vol32/iss4/2/. See also Cave, Stephen. "The Problem with Intelligence: Its Value-Laden History and the Future of AI." AIES '20: Proceedings of the AAAI/ACM Conference on AI, Ethics, and Society (2020): 29-35. https://dl.acm.org/doi/abs/10.1145/3375627.3375813.

[70] European Digital Rights (EDRI), Access Now, ARTICLE19, Bits of Freedom, the Chaos Computer Club (CCC), Digitale Gesellschaft CH, IT-Political Association of Denmark (IT-Pol). "Prohibit all Remote Biometric Identification (RBI) in publicly accessible spaces." *Joint civil society recommendations for an EU Artificial Intelligence Act for Fundamental Rights*. 2021. https://edri.org/wp-content/uploads/2022/05/Prohibit-RBI-in-publicly-accessible-spaces-Civil-Society-Amendments-AI-Act-FINAL.pdf.

[71] Access Now, European Digital Rights (EDRI), Bits of Freedom, ARTICLE19, IT-Pol. "Prohibit remote biometric categorisation in publicly accessible spaces, and any discriminatory biometric categorisation." *Joint civil society amendments to the Artificial Intelligence Act*. 2021. https://www.accessnow.org/cms/assets/uploads/2022/05/Amendments-to-the-AI-Acts-treatment-of-biometric-categorisation.pdf.

[72] Centre for Media, Technology and Democracy, Cyber Policy Exchange. "Submission to the House of Commons Standing Committee on Access to Information, Privacy and Ethics." 2022. https://www.ourcommons.ca/Content/Committee/441/ETHI/Brief/BR11889704/br-external/Jointly1-e.pdf; Tessono, Christelle. "Facial Recognition Technology in Canada: A Brief Overview of Harms and Potential Benefits." 2022. https://www.ourcommons.ca/Content/Committee/441/ETHI/Brief/BR11801593/br-external/TessonoChristelle-e.pdf; Stevens, Yuan. *Now You See Me?: Advancing Data Protection and Privacy for Police Use of Facial Recognition in Canada*. https://www.cybersecurepolicy.ca/now-you-see-me; Stevens, Yuan and Sonja Solomun. *Facing the Realities of Facial Recognition Technology: Recommendations for Canada's Privacy Act*. https://www.cybersecurepolicy.ca/frt-privacy-act.

[73] See e.g., Orvacec, Jo Ann, "Artificial Intelligence, Automation, and Social Welfare: Some Ethical and Historical Perspectives on Technological Overstatement and Hyperbole" *Ethical and Social Welfare* 13 (2019), https://doi.org/10.1080/17496535.2018.1512142; Abdurahman, J. Khadijah, "Birthing Predictions of Premature Death"; Zomignani Barboza, Júlia, Lina Jasmontaitė-Zaniewicz, and Laurence Diver, "Aid and AI: The Challenge of Reconciling Humanitarian Principles and Data Protection" in *Privacy and Identity Management. Data for Better Living: AI and Privacy*, eds. Michael Friedewald, Melek Önen, Eva Lievens, Stephan Krenn, Samuel Fricker (Springer: New York City, 2019). https://link.springer.com/chapter/10.1007/978-3-030-42504-3_11.

[74] Proposal for a Regulation of the European Parliament and of the Council Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts COM/2021/206, (EU AI Act), article 5(1)(c).

[75] See e.g., Isaak, Jim and Mina J. Hanna. "User Data Privacy: Facebook, Cambridge Analytica, and Privacy Protection." IEEE Journals & Magazine 51, 8 (2018): 56-59. https://ieeexplore.ieee.org/abstract/document/8436400.

[76] See e.g., Ferreira, Michelly Rosa and Luisa Agante. "The Use of Algorithms to Target Children while Advertising on YouTube Kids Platform: A Reflection and analysis of the existing regulation." *International Journal of Marketing, Communication and New Media* 8 (2020). http://u3isjournal.isvouga.pt/index.php/ijmcnm/article/view/457; 5Rights Foundation. "How data-hungry companies expose children to risk online: the case of recommendation systems." https://5rightsfoundation.com/in-action/how-data-hungry-companies-expose-children-to-risk-online-the-case-of-recommendation-systems.html.

[77] Tech Transparency Project. "Pills, Cocktails, and Anorexia: Facebook Allows Harmful Ads to Target Teens." May 4, 2021. https://www.techtransparencyproject.org/articles/pills-cocktails-and-anorexia-facebook-allows-harmful-ads-target-teens.

[78] Wells, Georgia, Jeff Horwitz, and Deepa Seetharaman. "Facebook Knows Instagram Is Toxic for Teen Girls, Company Documents Show." The Wall Street Journal. Dow Jones Company, September 14, 2021. https://www.wsj.com/articles/facebook-knows-instagram-is-toxic-for-teen-girls-company-documents-show-11631620739.

[79] EU AI Act, article 5(1)(a).

[80] EU AI Act, article 5(1)(b).

[81] Including data minimisation, data sharing, profiling, nudge techniques and geolocation. See Information Commissioner's Office. "Standards of age appropriate design." 2018. https://ico.org.uk/for-organisations/guide-to-data-protection/ico-codes-of-practice/age-appropriate-design-a-code-of-practice-for-online-services/standards-of-age-appropriate-design/.

[82] Information Commissioner's Office. "Standards of age appropriate design."

[83] Breiman, Leo, "Statistical Modeling: The Two Cultures (with Comments and a Rejoinder by the Author)", Statistical Science 16, no. 3 (January 2001), https://doi.org/10.1214/ss/1009213726.

[84] Goodfellow, Ian J., et al., "Explaining and Harnessing Adversarial Examples", International Conference on Learning Representations, 2015. http://arxiv.org/abs/1412.6572.

[85] Eykholt, Kevin, et al., "Robust Physical-World Attacks On Deep Learning Visual Classification", 2018 IEEE/CVF Conference On Computer Vision And Pattern Recognition, 2018, doi:10.1109/cvpr.2018.00175.

[86] Eckhouse, Laurel, et al., "Layers of Bias: A Unified Approach for Understanding Problems with Risk Assessment", Criminal Justice and Behavior 46, no. 2 (2018): pp. 185-209, https://doi.org/10.1177/0093854818811379.

[87] Ochigame, Rodrigo, "The Long History of Algorithmic Fairness", Phenomenal World, March 17, 2022, https://www.phenomenalworld.org/analysis/long-history-algorithmic-fairness/.

[88] Hoadley, Bruce, "Comment" [on Leo Breiman, "Statistical Modeling: The Two Cultures"], Statistical Science 16, no. 3 (January 2001), https://doi.org/10.1214/ss/1009213726.

[89] Kiviat, Barbara, "The Moral Limits Of Predictive Practices: The Case Of Credit-Based Insurance Scores", American Sociological Review 84, no. 6 (2019): 1134-1158, doi:10.1177/0003122419884917.

[90] Hellman, Deborah, When Is Discrimination Wrong? (Cambridge, Mass: Harvard University Press, 2011).

[91] Fourcade, Marion and Kieran Healy, "Classification Situations: Life-Chances in the Neoliberal Era", Accounting, Organizations and Society 38, no. 8 (2013): pp. 559-572, https://doi.org/10.1016/j.aos.2013.11.002.

[92] Fergus, Devin, "The Ghetto Tax: Auto Insurance, Postal Code Profiling, and the Hidden History of Wealth Transfer", In Beyond Discrimination: Racial Inequality in a Post-Racist Era, edited by Fredrick C. Harris and Robert C. Lieberman, 277–316, Russell Sage Foundation, 2013. http://www.jstor.org/stable/10.7758/9781610448178.15.

[93] Mason, Robert and Martha Butler, "Section 15 of the Canadian Charter of Rights and Freedoms: The Development of the Supreme Court of Canada's Approach to Equality Rights Under the Charter," Library of Parliament, Revised on September 1, 2021. https://lop.parl.ca/sites/PublicWebsite/default/en_CA/ResearchPublications/201383E

[94] Milke, Mark, "Myths and Facts about Automobile Insurance in Canada", report for the Insurance Bureau of Canada, December 27, 2006. https://www.dyckinsurance.ca/wp-content/uploads/2018/05/myths_about_auto_ins.pdf.

[95] Horan, Caley, Insurance Era: Risk, Governance, and the Privatization of Security in Postwar America (Chicago: The University of Chicago Press, 2021).