Brief on 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*

Submitted to the House of Commons Standing Committee
on Industry and Technology

by the
International Civil Liberties Monitoring Group

22 September 2023

International Civil Liberties Monitoring Group
#210-4 Florence Street, Ottawa, ON, K2P 0W7
national.coordination@iclmg.ca | http://iclmg.ca
(613) 241-5298

Introduction

The International Civil Liberties Monitoring Group (ICLMG) is a Canadian coalition of 45 organizations founded in 2002, following the adoption of Canada's first *Anti-terrorism Act*. Over the ensuing two decades we have worked with our members, partner organizations, impacted communities and law makers to defend civil liberties in Canada against national security over-reach and abuses in the name of countering terrorism.

The coalition's work regularly includes intervening on legislation and government policy of concern. This includes submitting briefs and appearing before parliamentary committees, including in regard to federal consultations on reforms to the *Privacy Act*,[1] the recent study on the use and impacts facial recognition technology by the House of Commons Standing Committee on Access to Information, Privacy and Ethics,[2] and the House Standing Committee on National Defense's study on cyberwarfare and cyberattacks.[3]

Concerns around protecting privacy, combatting surveillance and defending related rights have been central to our work. This includes organizing the International Coalition Against Mass Surveillance in 2005, researching and documenting the exponential growth of both government and private sector surveillance in the wake of 9/11 and the War on Terror, and engaging with parliamentarians on legislation to protect privacy rights, including opposing legislation that would undermine those rights.

In line with this work, we are providing commentary, including proposed revisions, regarding Bill C-27, the *Digital Charter Implementation Act*. Our submission will cover the following areas:

1. The Consumer Privacy Protection Act (CPPA)
    a. Recognizing privacy as a human right
    b. National security-related exemptions to consent must be removed
2. The Personal Information and Data Tribunal Act (PIDTA)
3. The Artificial Intelligence and Data Act (AIDA)
    a. Over-arching concerns
    b. Expanding scope of coverage of AIDA
    c. Definition of harms must be extended to include group-based harms
    d. Exclusion of national security related technology must be rescinded
    e. Need for independent oversight and review

Given that our expertise is not specifically on consumer privacy protection, there are areas of this bill that we will not comment on. We would emphasize, though, that our silence on certain sections does not signal support, given that we are aware that there are several other aspects of

[1] ICLMG, "Modernizing Canada's Privacy Act Consultation," 15 February 2021. Online at: https://iclmg.ca/wp-content/uploads/2021/10/Privacy-Act-consultation-submission-ICLMG.pdf
[2] ICLMG, "Brief: Study of the Use and Impact of Facial Recognition Technology," 13 April 2022. Online at: https://iclmg.ca/wp-content/uploads/2022/04/ICLMG-brief-to-ETHI-FRT-study.pdf
[3] ICLMG, "Submission to the Standing Committee on National Defence for its study on Cybersecurity and Cyberwarfare," 6 April 2023. Online at: https://iclmg.ca/wp-content/uploads/2023/04/NDDN-submission-re-cybersecurity-and-cyberwarfare.pdf

this bill that privacy, consumer rights, human rights and civil liberties organizations are raising concerns over. We hope that our contribution to your study of C-27 will help complement that broader discussion.

1. The *Consumer Privacy Protection Act* (CPPA)

a. Recognizing privacy as a human right

It is fundamental that Canada formally recognize the right to privacy as a human right. It is laudable that the Preamble of Bill C-27 recognizes that privacy is essential to "individual autonomy and dignity and to the full enjoyment of fundamental rights and freedoms in Canada." However, inclusion in the preamble doesn't go far enough since the preamble does not remain a part of the legislative regime once the bill is adopted.

There is extensive precedent in Canadian and international law for the explicit recognition of privacy as a human right.

First, rulings by the Supreme Court of Canada have recognized that privacy rights maintain quasi-constitutional status in Canada.[4] The Office of the Privacy Commissioner of Canada has also stated clearly that the "freedom to live and develop free from surveillance is a fundamental human right," and that "individuals must be able to navigate public, semi-public, and private spaces without the risk of their activities being routinely identified, tracked and monitored."[5]

Beyond this recognition in Canadian law and jurisprudence, the right to privacy is also recognized in international accords, including fundamental agreements to which Canada is a long-standing signatory.

Article 17 of the International Covenant on Civil and Political Rights states that:

> 1. No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation.
>
> 2. Everyone has the right to the protection of the law against such interference or attacks.[6]

This has been interpreted by the UN Human Rights Committee as requiring not only protection from state surveillance, but from all other legal or natural persons as well.[7]

---

[4] *Lavigne v. Canada (Office of the Commissioner of Official Languages)*, [2002] 2 S.C.R. 773, at para. 24.
[5] Office of the Privacy Commissioner, "Draft privacy guidance on facial recognition for police agencies" (2021) at para 9. Online at: www.priv.gc.ca/en/about-the-opc/what-we-do/consultations/gd_frt_202106/
[6] International Covenant on Civil and Political Rights, 16 December 1966, General Assembly resolution 2200A (XXI). Online at: https://www.ohchr.org/en/instruments-mechanisms/instruments/international-covenant-civil-and-political-rights
[7] Scassa, Teresa (2020). A Human Rights-Based Approach to Data Protection in Canada. [S.l.] : SSRN. https://ssrn.com/abstract=3620450.

As privacy expert Teresa Scassa notes:

> Freedom of association, limits to disproportionate surveillance practises, and prevention of discrimination based on sensitive personal data are just few examples of the social effects of safeguarding the right to privacy and personal information. Values such as democracy and pluralism are strictly related to the protection of these rights. (p. 245) A human rights-based approach to privacy not only recognizes a fundamental right to privacy, but also acknowledges the interrelationship between privacy and the right of individuals to exercise their other rights and freedoms with autonomy and dignity. Further, the human right to privacy must be supported by legislation that renders the right effective and realizable.[8]

Despite the fact that the fundamental nature of privacy rights has been recognized in the courts, among officers of Parliament, and by international treaty bodies, its absence from Bill C-27 presents a significant gap. Privacy as a human right must be explicitly included in legislation to provide it with the legal weight it deserves. This is particularly important in Bill C-27, which regulates the protection of consumer privacy rights and the activities of the private sector.

By failing to recognize privacy as a human right in Bill C-27, the balancing in determining the appropriate collection, retention and use of personal information is based on the interests of private corporations versus individuals' privacy interests. The result is that economic interests will likely trump the privacy interests of individuals, since it will not be backed in the law with the weight of recognition of privacy as a human right.[9]

Recommendation 1: Recognize privacy as a fundamental right in the text of Bill C-27

Proposed amendment:
5 The purpose of this Act is to establish — in an era in which data is constantly flowing across borders and geographical boundaries and significant economic activity relies on the analysis, circulation and exchange of personal information — rules to govern the protection of personal information in a manner that recognizes the fundamental right to ~~of~~ privacy of individuals…

b. National security-related exemptions to consent must be removed

We are deeply concerned that Bill C-27 maintains overly-broad exceptions to consent when it comes to the collection, retention, use and disclosure of personal information for national security reasons.

[8] Ibid.
[9] OpenMedia, "Submission to INDU Committee Study of Bill C-27, The Digital Charter Implementation Act, 2022," 3 May 2023. Online at: https://openmedia.org/assets/Bill_C-27_Submission_-_OpenMedia.pdf [*OpenMedia 2023]*

This includes section 47, which allows a government agency to request disclosure of personal information from private entities solely on the grounds that it "suspects that the information relates to national security, the defence of Canada or the conduct of international affairs," as well as section 48, which allows private entities to collect, use and disclose personal information to government agencies if it "suspects that the information relates to national security, the defence of Canada or the conduct of international affairs."

First, such provisions contradict the purpose of Bill C-27 as stated in s. 5 as well as the "appropriate purposes" clause in s. 12(1).

Section 5 states that the bill sets out rules in a manner that protects the right to privacy of individuals and the need for organizations to "collect, use or disclose personal information for purposes that a reasonable person would consider appropriate in the circumstances." Section 12(1) states, "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…"

While sections 30 (Emergency Use), 43 (Institutions Administering law — request of government institution), and 44 (Law enforcement — request of government institution) all allow for the disclosure of personal information without consent, they set out reasonable justifications: responding to an emergency, administering a federal or provincial law, or carrying out an investigation in order to enforce a federal or foreign law. Government departments must demonstrate their lawful authority to request such information, and the exceptions are limited to disclosure.

Even section 45, which creates a broader exception allowing for private entities to disclose of their own initiative personal information relating to the contravention of a law, requires that the private entity must meet the standard of **reasonable grounds to believe** "that the information relates to a contravention of federal or provincial law or law of a foreign jurisdiction that has been, is being or is about to be committed."

Each of these could be argued to meet the reasonableness standard, given the specific circumstances, and the inclusion of appropriate (if minimal) safeguards.

However, s. 47 (1) allows for the disclosure of personal information without consent upon the request of a government agency solely on the grounds that the agency "**suspects** that the information relates to national security, the defence of Canada or the conduct of international affairs." This is a much weaker standard than what is provided in sections 30, 43 or 44.

Moreover, sections 47 (2) and (3) also empower private entities to collect and use personal information without consent for the purposes of 47 (1), again going much further than other similar sections. This clearly goes beyond what should be considered "reasonable" or "acceptable" use of personal information. There is also no justification for a broader exemption simply because of concerns related to "national security, defence or international affairs." Allowing s. 47 to remain would result in a regime that allows government agencies to obtain information in secret from private entities on poorly defined grounds based only on "suspicion that the information relates to national security, the defence of Canada or the conduct of

international affairs." This raises not only significant privacy concerns, but concerns around abuse in terms of overly-broad data collection and surveillance of individuals and communities based only on "suspicion of relating to national security" rather than on grounds to believe it is related to a contravention of federal or provincial law.

Section 48 raises even more significant concerns: s. 48 (1) allows private entities, of their own accord, to disclose personal information, without consent, to government agencies, again on the basis of "national security, the defence of Canada or the conduct of international affairs." However, unlike section 45, concerning disclosure of information relating to the contravention of a federal law, the private entity must only **suspect** that the disclosed information relates to national security – much lower than the "reasonable grounds to believe" threshold set out in section 45.

Similar to section 47, section 48 goes on to include clauses (2) and (3) which allow for the private entity to also collect and use personal information for the purposes of section 48 (1). The result is that a private entity would be able to collect, use and disclose personal information without consent, based only on suspicion that it relates to national security, defence or international affairs. Given the incredibly broad nature of "national security" alone, and the long history of the use of national security to justify the inappropriate and unlawful surveillance and criminalization of various communities in Canada, it is impossible to see how this can be considered a reasonable or appropriate purpose. In fact, it can be reasonably foreseen to result in the over-collection and over-sharing of personal information with government agencies, resulting in violations of not just privacy rights, but also associated freedoms of expression, assembly and equality rights.

Recommendation 2: That section 47 be removed from the CPPA, or in the alternative, be amended to meet the threshold of reasonable grounds to believe, and be restricted to disclosure.

Proposed amendment (a):
Remove s. 47(1) to (3) in its entirety

OR Proposed amendment (b):
47 (1) An organization may disclose an individual's personal information without their knowledge or consent to a government institution or part of a government institution that has made a request for the information, identified its lawful authority to obtain the information and indicated that it has reasonable grounds to believe ~~suspects~~ that the information relates to an imminent threat to national security, the defence of Canada or the conduct of international affairs.

~~(2) An organization may collect an individual's personal information without their knowledge or consent for the purpose of making a disclosure under subsection (1).~~

~~(3) An organization may use an individual's personal information without their knowledge or consent if it was collected under subsection (2).~~

Recommendation 3: That section 48 be removed from Bill C-27, or, in the alternative, meet the threshold of reasonable grounds to believe, and be restricted to disclosure.

Proposed amendment (a):
Remove s. 48 (1) to (3) in its entirety

OR Proposed amendment (b):
48 (1) An organization may on its own initiative disclose an individual's personal information without their knowledge or consent to a government institution or a part of a government institution if the organization has reasonable grounds to believe ~~suspects~~ that the information relates to an imminent threat to national security, the defence of Canada or the conduct of international affairs.

~~(2) An organization may collect an individual's personal information without their knowledge or consent for the purpose of making a disclosure under subsection (1).~~

~~(3) An organization may use an individual's personal information without their knowledge or consent if it was collected under subsection (2).~~

2. The *Personal Information and Data Tribunal Act*

It is essential that, if Canada's private sector privacy laws are to be appropriately respected, the body tasked with overseeing privacy protections in Canada be granted adequate powers. We therefore welcome the creation of new order-making powers for the Office of the Privacy Commissioner of Canada (OPC) in the CPPA, to compel private entities to:

- take measures to comply with the CPPA
- stop actions that contravene the CPPA
- comply with the terms of a compliance agreement
- make public any measures taken or proposed to be taken to correct the policies, practices, or procedures that the entity has put in place to fulfill its obligations under the CPPA

Moreover, the CPPA would allow for the OPC to impose Administrative Monetary Penalties (AMPs) on entities found to be non-compliant.

These are all important and necessary improvements in the powers of the OPC to ensure that privacy rights in Canada are protected and that privacy regulations are respected.

However, we share concerns that the proposed Personal Information and Data Tribunal proposed in part two of Bill C-27 will only serve to undermine these new powers.[10] We join others in noting that the ability of the Tribunal to approve AMPs and decide on appeals of orders and

[10] OpenMedia 2023

penalties undermines not just the powers of the OPC, but the independence of the process. The Privacy Commissioner is a fully independent officer of parliament, appointed upon consultation with other parties. The members of the Tribunal, though, are appointed by the Governor in Council, upon recommendation of the relevant Minister, opening the possibility of a less independent body deciding appeals of an independent officer's orders.

Further, as the OPC points out, "provincial counterparts with substantially similar private sector privacy legislation do not have this type of administrative tribunal acting as a review body."[11] Research from OpenMedia has also shown that similar jurisdictions such as the United Kingdom, European Union, New Zealand, and Australia have also forgone a tribunal to review the work of their privacy officials.[12]

Recommendation 4: That the *Personal Information and Data Tribunal Act* be removed from Bill C-27, in favor of a process whereby orders can be directly appealed to the Federal Court of Canada.

Proposed amendment:
Strike *Part 2: The Personal Information and Data Tribunal Act* from Bill C-27.

3. The *Artificial Intelligence and Data Act*

a. Over-arching concerns

Through our work, we have documented how a lack of regulation of artificial intelligence tools and how they are used can have significantly negative impacts on the rights and livelihoods of people in Canada and internationally. This includes its use to power surveillance tools, to categorize individuals, to attempt to predict unlawful activity or to make potentially life-altering decisions in a wide-range of sensitive areas, including employment, immigration, border security, law enforcement, and intelligence gathering.

We are particularly aware of the interest among government, law enforcement and intelligence agencies to harness AI tools, and to work with private contractors developing those tools, for counter-terrorism and national security purposes. We have also seen how such tools can be used to violate fundamental rights and can either be shared with, sold to, leaked, or stolen by a wide range of actors who can use the tools for their own nefarious purposes.

Given all this, we are acutely aware of the need to regulate the development and use of AI tools in the private sector. However, after evaluating the proposed Artificial Intelligence and Data Act (AIDA), we do not believe that it is fit to serve this purpose.

[11] Office of the Privacy Commissioner of Canada, "Submission of the Office of the Privacy Commissioner of Canada on Bill C-27, the Digital Charter Implementation Act, 2022," April 2023. Online at: https://www.ourcommons.ca/Content/Committee/441/INDU/Brief/BR12370320/br-external/OfficeOfThePrivacyCommissionerOfCanada-brief-e.pdf
[12] OpenMedia 2023

In particular, as previously expressed in a letter to the government and party leaders,[13] we maintain the following reservations about AIDA:

- Numerous key aspects of the Act are left to regulation, and will be decided on only after it is passed. This will result in less scrutiny and transparency.
- The proposed oversight mechanism is arbitrary, and the enforcement mechanism is fragile, including a lack of independence for the proposed AI and Data Commissioner.
- The Act fails to apply to government institutions, including national security agencies. This opens the door to abuses by law enforcement agencies like the Royal Canadian Mounted Police's (RCMP) unlawful use of Clearview AI's facial recognition technology.
- The Act does not address the significant human rights implications of algorithmic systems.
- As part of a larger study of C-27, AIDA will not receive the necessary degree of scrutiny that it requires.
- The committee cannot engage in the level of public consultation that is necessary to address the flaws in this bill and which the government should have undertaken before tabling legislation.
- Key amendments necessary for addressing the flaws in the Act would be deemed to go beyond what is possible at committee, for example applying the Act to government institutions or establishing an adequate, independent oversight body.

For all these reasons, we recommend that the committee remove AIDA from Bill C-27 in favour of a more robust, transparent and public consultation on how best to regulate artificial intelligence in Canada and to bring stronger legislation back to Parliament once it is developed.

Recommendation 5: That the committee remove AIDA from Bill C-27 in favour of a more robust, transparent and public consultation on how best to regulate artificial intelligence in Canada and to bring stronger legislation back to Parliament once it is developed.

However, we are also cognizant that at this stage AIDA may very well be adopted. While we do not believe that the Act can be sufficiently amended to truly address the fundamental problems with the Act, we make the following suggestions in order to address some key concerns.

b. Expanding scope of coverage of AIDA

Currently, the regulatory framework proposed by AIDA would only apply to "high impact systems." In a reflection of a problem throughout AIDA, "high impact system" is not defined in the Act, and it left instead for regulation. This raises several deep concerns:

First, without a clear definition of a high impact system, it is impossible to evaluate what technology would fall under the scope of this Act. This undermines the ability for both the public

[13] "Letter to party leaders urging vote against AIDA at second reading," 14 March 2023. Online at: https://iclmg.ca/vote-against-aida/

and parliamentarians studying this bill to be certain that the proposed regime will be adequate and effective.

Second, by leaving the definition to regulations alone, the process of defining "high impact" eludes the transparency and rigour of study by parliament. Regulations are often adopted without the same level of scrutiny of a bill, and could lead to the further obscuring of a process that has already suffered from a lack of transparency and consultation.

Third, while regulations provide flexibility, to leave such a key definition underpinning the entire framework of AIDA to such a process could result in the weakening of the regulatory framework in the future.

Additionally, the limiting of AIDA to regulating "high impact systems" is in itself a concern. While it is clear that "high impact systems" must be regulated, the Act is silent on AI systems that present other degrees of harm. This would mean that the multitude of types of AI systems, which present a wide range of impacts, would be expected to be divided neatly into two categories. This will likely present substantial challenges in the future as it will likely already face severe challenges in addressing generative AI systems. Not only that, but this approach is also out of step with other jurisdictions such as the EU. For example, the proposed EU AI Act would establish four clear categories of AI systems, each with a progressing degree of regulation:

- Unacceptable risk
- High Risk
- Generative AI
- Limited Risk

"Unacceptable risk" would be AI systems that present such an unmitigable risk to rights that it must be banned; "high risk" would require substantial analysis and assessment before use; and "limited risk" would still be required to meet requirements around transparency and user consent.[14]

We would recommend that the committee amend AIDA to include escalating categories of AI systems requiring regulation, modeled after the definitions included in the EU *AI Act*. We would further recommend that new categories be allowed to be added by regulation, as necessary, in order to preserve the ability to adapt the regulatory framework when needed, but to still maintain a minimum level of regulation.

Finally, AIDA also falls short in defining how an AI system is categorized as "high impact." Section 7 allows for such a determination to simply be made by "a person who is responsible for an artificial intelligence system." It is essential that, in order to assess the level of impact of an AI system, independent and clear criteria be established. We support the recommendation by LEAF in their submission on AIDA that an assessment "must include performing an equity and

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

privacy audit as prescribed by regulation," as well as other related amendments which we include below.[15]

Recommendation 6: That AIDA be amended to include categories of AI systems beyond "high impact systems," to include non-exhaustive definitions of what levels of risk are captured by each category, and to ensure that such categorization is predicated on the performance of an equity and privacy audit. (NB: Proposed amendments (b) and (c) are based primarily on proposals in LEAF's brief, pp. 11 & 13)

Proposed amendment (a):
5 (1) The following definitions apply in this Part.
…
Unacceptable system means… [insert definition]
High impact system means… [insert definition]
Low impact system means… [insert definition]

Proposed amendment (b):

- Remove s. 7 and remove "high-impact" from ss. 8, 9, 11, 12.

Proposed amendment (c):
8 A person who is responsible for an ~~high-impact~~ AI system must, in accordance with the regulations, establish measures to identify, assess and mitigate the risks of harm or biased output that could result from the development or use of the system. This must include performing an equity and privacy audit as prescribed by regulation.

11 (1) A person who makes available for use ~~a high-impact system~~ an AI system must, in the time and manner that may be prescribed by regulation, publish on a publicly available website a plain-language description of the system that includes an explanation of
(a) how the system is intended to be used;
(b) the types of content that it is intended to generate and the decisions, recommendations or predictions that it is intended to make;
(c) the results of an equity and privacy audit as prescribed by regulation**;** …

36 The Governor in Council may make regulations for the purposes of this Part, including regulations:
(b) establishing criteria for the ~~definition *high-impact system*~~ purpose of further defining or the addition of further categories of AI systems in in subsection 5(1);
(x1) establishing criteria for the oversight and management of AI-systems by persons responsible;
(x2) outlining the requirements for equity and privacy audits of AI systems.

[15] Kim, Rosel and Thomasen, Kristen, Submission to The Standing Committee on Industry and Technology on 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 (September 11, 2023). At pp. 11, 13. Available at SSRN: https://ssrn.com/abstract=4571389 [LEAF 2023]

c. Definition of harms must be extended to include group-based harms

Currently, the definition of harms in AIDA is limited to individual harms related to physical or psychological harm, damage to property and economic loss. This definition ignores the documented reality of artificial intelligence causing group-based harms by infringing on collective rights. As explained by LEAF:

"Collective rights are those held by a group as a whole, in contrast to individual rights which are held individually by members of the group. Collective rights protect the interests of a group, such as cultural and language rights, collective privacy, environmental rights, and labour and union rights, all of which are significantly threatened by the introduction of AI systems."[16]

There are numerous ways in which collective and group rights are or can be impacted by artificial intelligence tools. In regards to national security, this includes the selection and categorization of individuals based on assessed risk for the purposes of immigration, employment, travel or even surveillance. It also includes the use of artificial intelligence systems to surveil and investigate entire groups based on criteria programed into the AI tool, as well as the harms visited upon entire groups who face the repercussion of biased systems that have difficulty identifying people of certain races, ages or genders. It can also be used to determine (and exclude) categories of individuals for financial services. Outside of national security, collective harms can also come in the form of other human rights violations, employment violations, IP right violations, etc.[17]

We once again support the recommendation from LEAF on this issue, namely that s. 5 should be amended to account for collective harms.[18]

Recommendation 7: Amend s. 5 to expand the definition of harms to include collective harms.

Proposed amendment:
5 (1) "Harm means
(a) physical or psychological harm to an individual or identifiable group;
(b) damage to an individual's property, collectively owned property, land or buildings held on behalf of a group or collective, or public property or public spaces; or
(c) economic loss to an individual or identifiable group."

[16] LEAF 2023, p.6
[17] See, Blair Attard-Frost, "Generative AI Systems: Impacts on Artists & Creators and Related Gaps in the Artificial Intelligence and Data Act - Submission to the Standing Committee on Industry and Technology" (5 June 2023) at 13, online: House of Commons https://www.ourcommons.ca/Content/Committee/441/INDU/Brief/BR12541028/br-external/AttardFrostBlair-e.pdf; LEAF 2023; Bailey, J., Burkell, J., and McPhail, B. "Submissions on Bill C-27: The Digital Charter Implementation Act," September 2023.
[18] LEAF 2023, p.5

d. Exclusion of national security related technology must be rescinded

Internationally, we have seen the exponential growth in interest in using artificial intelligence tools for counterterrorism and national security purposes. This includes: monitoring for terrorism content online; engaging in surveillance; analysing retained data to identify trends and predict terrorist activities; facilitating and guiding remote and autonomous weapons; and rendering decisions and/or categorizing individuals and groups according to risk in regards to immigration, employment and travel.

Each of these engenders the possibility of some of the most serious risks to individuals' rights, including freedom of expression, freedom of association, freedom of movement, security of the person, equality rights, privacy rights and more.

Canadian national security agencies like the RCMP, CBSA, CSIS and CSE have been open regarding their interest and use of artificial intelligence tools for a wide range of purposes, including for facial recognition, for surveillance, for border security, for data analytics and for cybersecurity. However, they have not revealed the specific ways in which they use artificial intelligence systems, nor what steps they are taking to mitigate harm. Moreover, no clear framework has been established to regulate their use of these tools in order to prevent serious harm to individuals or to groups.

AIDA presents an opportunity to address this gap, by regulating private sector technology used by these national security agencies. It is shocking, then, that in s. 3 (2), AIDA goes in the opposite direction and explicitly excludes the application of the Act to:

> …a product, service or activity that is under the direction or control of
> (a) the Minister of National Defence;
> (b) the Director of the Canadian Security Intelligence Service;
> (c) the Chief of the Communications Security Establishment; or
> (d) any other person who is responsible for a federal or provincial department or agency and who is prescribed by regulation.

This would mean that any AI system developed by a private sector actor which falls under the direction or control of the government would face absolutely no independent regulation or oversight. Such an exclusion is completely unacceptable.

As the UN Special Rapporteur on Counterterrorism and Human Rights reported to the UN Human Rights Committee in March 2023, "The Special Rapporteur is deeply concerned with the entrenched practice of States adopting legislation that exempts the use of AI for military and national security purposes from ordinary oversight regimes."[19]

[19] "Human rights implications of the development, use and transfer of new technologies in the context of counter-terrorism and countering and preventing violent extremism," Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, Fionnuala Ní Aoláin. Human Rights Council, Fifty-second session, A/HRC/52/39, 1 March 2023. Online at https://www.ohchr.org/sites/default/files/documents/issues/terrorism/sr/reports/A-HRC-52-39-AdvanceEditedVersion.docx. [SR 2023]

The report goes on to note:

"She [the Special Rapporteur] draws attention to the ways in which security imperatives and counter-terrorism rationales are used to validate the development, use and transfer of new technologies, including, but not limited to, biometric technologies, AI, unmanned aerial vehicles (drones) and surveillance tools. She decries the ways in which, under the guise of preventing terrorism, new technologies have been used that, in practice, function to profoundly undermine the rights of individuals and communities. High-risk technologies have been brought in through the proverbial "back door", validated by appeals to security that in actuality weaken broader collective security and undermine the promotion and protection of human rights."[20]

In providing the example of the EU *AI Act*, she further stressed, "that AI systems developed for military or dual-use purposes should be regulated by the AI act. She maintains the position that the Council of Europe convention must include the design, development and use of AI systems for national defence within its ambit. To exclude them would effectively make the proposed convention irrelevant to the human rights concerns that are of greatest relevance in the region."[21]

Similar concerns directly apply to AIDA's exclusion of AI systems developed for use by Canadian national security agencies. All AI systems developed by the private sector must face regulation, regardless of its use by national security agencies. While the government may argue that should this technology be sold on the private market, it would then be regulated, it ignores the severe impact that unregulated technology used by these agencies could, and certainly will, have. It also ignores that such technology could be leaked or hacked, or potentially developed for a Canadian agency and then sold in markets without stringent AI regulations. Moreover, we would be concerned that allowing for unregulated development for government use would lead to pressure to weaken regulations around the eventual re-packaging of such technology for the private sector.

Recommendation 8: Strike s. 3(2) from AIDA

Proposed amendment:

~~Product, service or activity~~

~~3 (2) This Act does not apply with respect to a product, service or activity that is under the direction or control of~~

~~(a) the Minister of National Defence;~~

~~(b) the Director of the Canadian Security Intelligence Service;~~

~~(c) the Chief of the Communications Security Establishment; or~~

~~(d) any other person who is responsible for a federal or provincial department or agency and who is prescribed by regulation.~~

[20] Ibid.
[21] Ibid.

e. Need for independent oversight and review

As it currently stands, the enforcement of AIDA and development of related regulations falls to the Minister of Innovation, Science and Economic Development, who may delegate all powers (save regulation making powers) to a senior official of the department designated as the Artificial Intelligence and Data Commissioner.

This should be revised in favor of establishing an independent officer of parliament, outside of ISED, in order to oversee the administration and enforcement of AI regulations. It is inappropriate that this position falls under the purview of ISED, whose mandate includes the promotion of the AI industry. It is unavoidable that at times the need for regulation will conflict with the interests of the AI industry; it is crucial that in those instances there is an independent regulator not subject to this potential conflict of interest (or even the appearance of such a conflict).

We would therefore recommend that AIDA be amended to allow for the creation of an independent regulator:

- The AI and Data Commissioner is appointed by the Governor in Council after consultation with senate and house of commons opposition leaders and approval of the appointment by resolution of the Senate and House of Commons.
- The Commissioner's role is the administration and enforcement of this Part
- That the Commissioner be given the rank of deputy head
- That they be granted the power to appoint or lay off employees, require appropriate security clearance, etc.

The remainder of AIDA would then be amended to, in the appropriate sections, replace "Minister" with "AI and Data Commissioner".

Alternatively, section 33(2) could be amended to simply allow for the creation of an independent officer; however, this would still fall short of ensuring that an independent regulator will be created, and that they would not serve at the discretion of the ISED Minister.

Recommendation 9: That AIDA be amended to create an independent Artificial Intelligence and Data Commissioner who would oversee the administration and enforcement of the Act.

Proposal (a):

- Amend s. 32 to include:
    - The AI and Data Commissioner is appointed by the Governor in Council after consultation with senate and house of commons opposition leaders and approval of the appointment by resolution of the Senate and House of Commons.
    - The Commissioner's role is the administration and enforcement of this Part
    - That the Commissioner be given the rank of deputy head
    - That they be granted the power to appoint or lay off employees, require appropriate security clearance, etc.

(continued)

- Amend the remainder of AIDA, including s. 13 to 21, to place enforcement and administration powers under the purview of the Commissioner

Proposal (b)

- Amend 33(2) to allow for the creation of an independent regulator
- Amend the remainder of AIDA, including s. 13 to 21, to place enforcement and administration powers under the purview of the independent regulator

It will also be essential that, over time, the provisions of AIDA be evaluated for effectiveness and impact. AIDA will also need to be re-evaluated given the certainty of new developments withing the AI field that, despite attempts at "future-proofing," will require amendments to the Act. To accomplish this, the Act should include provisions for both annual reporting and periodic reviewing of the Act.

Recommendation 10: That AIDA be amended to require annual public reporting and a five-year review of the Act

Proposed amendments:

Reporting

38 The Artificial Intelligence and Data Commissioner (Commissioner) shall, within three months after the termination of each financial year, submit an annual report to Parliament on the activities of the office during that financial year.

39 The Commissioner may, at any time, make a special report to Parliament referring to and commenting on any matter within the scope of the powers, duties and functions of the Commissioner where, in the opinion of the Commissioner, the matter is of such urgency or importance that a report thereon should not be deferred until the time provided for transmission of the next annual report of the Commissioner under section 38.

40 (1) Every report to Parliament made by the Commissioner under section 38, 39, 41 or 42 shall be made by being transmitted to the Speaker of the Senate and to the Speaker of the House of Commons for tabling in those Houses.

(2) Every report referred to in subsection (1) shall, after it is transmitted for tabling pursuant to that subsection, be referred to the committee designated or established by Parliament for the purpose of subsection 75(1).

(continued)

41 (1) The Commissioner shall, within three months after the termination of each financial year, submit a confidential report to the Minister containing information relating to the activities of the office that could not be divulged publicly

(2) Within thirty days of submitting this report, a summary of the report shall be tabled in Parliament

42 (1) The Commissioner may, at any time, make a special confidential report to the Minister referring to and commenting on any matter within the scope of the powers, duties and functions of the Commissioner where, in the opinion of the Commissioner, the matter is of such urgency or importance that a report thereon should not be deferred until the time provided for transmission of the next annual report of the Commissioner under section 41.

(2) Within thirty days of submitting this report, a summary of the report shall be tabled in Parliament

43 Any confidential report relating to matters of national security shall also be transmitted to the National Security and Intelligence Committee of Parliamentarians and the National Security and Intelligence Review Agency

Review

44 (1) Every five years beginning on the day on which this Act comes into force, the administration and operation of this Act shall be reviewed by the committee of the House of Commons, of the Senate or of both Houses that is designated or established for that purpose.

(2) The Minister must cause a report responding to the committee's review to be laid before each House of Parliament within 90 days after the receipt of the committee's report.

(3) If the Committee report identifies any deficiencies in the application of this Act the Minister's report must include a plan to remedy those deficiencies — including any proposed legislative amendments — and a timeline for its implementation.

**Renumber ensuing sections of the Act*