AI Governance & Safety Canada
Gouvernance et sécurité de l’IA Canada

March 1st, 2024

Mr. Joël Lightbound, M.P.
Chair
Standing Committee on Industry and Technology
House of Commons
Parliament of Canada

Dear Mr. Lightbound,

Further to our brief submitted on November 3rd, to the Minister’s amendments shared on November 28th, and to our oral testimony on January 29th, we are providing the committee with our updated recommendations for Bill C-27’s AI & Data Act.

The Minister’s amendments represent a good step in the right direction, and with a few remaining changes the Bill will be able to deliver significant protection for Canadians.

As discussed in detail in our initial brief: with frontier labs racing to build smarter-than-human AI and existing AI harms already being felt, Canadians do not have the luxury of waiting for another bill. Canada needs working legislation now.

We continue to urge committee members to not give up on the AI & Data Act, but to take the time to understand the full range of AI risks to be addressed, and prepare legislation that can serve Canadians well today and in the coming years.

We remain available for any assistance that you require.

Sincerely,

Wyatt Tessari L'Allié
Founder & Executive Director
AI Governance & Safety Canada
contact@aigs.ca

Feedback on the Minister’s amendments and updated recommendations for the AI & Data Act

Second brief to the Standing Committee on Industry and Technology on Bill C-27

March 1st, 2024

Table of contents

Feedback on the Minister’s amendments

The amendments submitted by the Minister on November 28th are commendable, suggest that stakeholder feedback was taken seriously, and represent a significant improvement to the AIDA. Per the five areas of interest outlined in the Minister’s document, we provide here the amendments we support and the *ones to reconsider*:

- **Defining high-impact systems**
    - Defining the risk categories in a schedule that can be updated by regulations, and allowing for distinct regulations for each category: This is a very elegant solution. It is better than using the fixed categories we had initially proposed, and will make the Act more future-proof.
    - *Limiting the Schedule (and by extension the definition of high-impact) to Use Cases*: As noted in our initial submission, there are some AI capabilities that present high or unacceptable risks regardless of the use case (e.g. unprompted self-modification, or active deception). These can be present in both general-purpose and single-purpose systems, as well as at the R&D stage before there is a clear use case. It is therefore essential for the Schedule to address both use cases and capabilities.

- **Aligning AIDA with EU AIA and OECD Definitions**
    - Aligning the AIDA definition of artificial intelligence with that of the OECD makes sense.
    - *Specifying that the Act only applies to AI systems or models that are placed on the market or put into use in the course of international or interprovincial trade*: This is a key weakness of the EU AIA and should not be copied. As outlined in our initial submission, the weaponisation, cybervulnerability, and control problems of AI systems arise at the R&D stage before they are commercialised. Moreover, the sole focus on commercial AI leaves Canada vulnerable to open source development which is an increasingly big player in the sector.
    - Clarifying how obligations would apply to AI systems that have been substantially modified is a good amendment. Relatively small edits to AI systems can lead to significant changes in their behaviour and risk profile, so having this clause will force AI developers and deployers to do their due diligence.
    - Explicitly requiring robust accountability frameworks: this is a very good idea, and can be complemented with a liability clause such as s.3 & 93 of Quebec’s Loi 25 to specify who exactly is responsible.

- **Establishing Clearer Obligations Along the AI Value Chain**
    - Separate requirements for entities at different stages of the AI value chain: Makes sense. The EU AIA takes a similar approach, albeit using different stages.
    - *Defining those stages and their specific requirements in the text of the Act*: In a rapidly evolving sector, regulators will need the flexibility to update the list of which entities in the AI value chain need to be regulated and how. Instead of putting this in the text of the Act, we recommend listing them in a Schedule (as

    the Minister proposed for the high-impact categorisation), and allowing tailored requirements for each. This will also address the need to include AI hardware and infrastructure providers in the Act, as discussed in our initial submission.

  - Requiring that operators notify users when they are interacting with an AI system: This is essential for dealing with deepfakes. While section 6(1) is limited in scope, it can be complemented by the clauses in 7 to 12 that allow additional regulation.
  - Granting the regulator the authority to make “cease operations” orders. This is an essential tool for government to adequately protect Canadians, and likely a far more effective mechanism to ensure compliance than administrative fines.

- **Obligations for General-Purpose Systems**
  - Specific requirements for general-purpose systems: this is essential, as GPAIS present a fundamentally different risk profile than single-purpose systems.
  - Section 7 and 8: these requirements appear proportionate and robust, especially given clause (h) which gives the regulators flexibility to add anything missing, such as licensing requirements, public consultations, or cybersecurity measures.

- **Strengthening and Clarifying the Role of the AIDC**
  - Granting enhanced powers to:
    - conduct investigatory activities,
    - compel the production of an organisation’s accountability framework,
    - determine whether a system or model falls within the scope of AIDA,
    - conduct or order the conduct of audits,
    - investigate where they have reasonable grounds to believe that an organisation has contravened or is likely to contravene their obligations,
    - enter premises, access systems, copy data, and conduct testing of AI systems,
    - require audited organisations to provide information and assistance,
    - enter into information sharing arrangements with relevant commissions and agencies

    These are all valuable tools for the AIDC to protect Canadians.
  - *Leaving the Governor in Council as the sole authority to make meaningful regulations*: the speed of AI developments and deep expertise required are incompatible with requiring the review and approval of Cabinet (which also introduces political interference). This is why we recommended creating a Commission like the CNSC which would have the capacity, knowledge and greater independence from political influence to regulate AI effectively. If this isn’t feasible, then the AIDC should be given this authority but with added oversight.
  - *Providing no independent oversight of the Minister’s or Commissioner’s powers*: The stakes around AI, and the risks of conflict of interest with ISED’s mandate to boost innovation, are too high to have the Industry Minister and their chosen AIDC perform this work without oversight. We recommend adding a separate oversight office based in parliament to monitor the administration of the Act, and/or to create an independent Ministry of AI.

Summary: the top 5 remaining changes needed

We recognise that the Act is in a late stage of the review process, and that the Minister's amendments already made significant strides towards improving it. We have therefore adapted the recommendations from our initial submission into a "top 5" most important remaining changes needed in the Act, in a manner to make the edits simple and achievable:

1) Expand the "high-impact systems" definition and schedule to include both use cases and capabilities	*Some AI capabilities present high or unacceptable risks regardless of the use case (e.g. unprompted self-modification or active deception). These can be present in both general-purpose and single-purpose systems, as well as at the R&D stage before there is a clear use case. Adjusting the wording of the schedule to include capabilities is essential to fill dangerous gaps.*
2) Remove the exemptions for government, national security, political parties, and open source	*Canada needs a unified and coherent approach to governing AI. Each of the currently exempted categories present significant risks and needs to be included in the Act. In particular, open source AI development is too big a phenomenon for the AIDA not to address. Due to the inherent difficulties in regulating its development and misuse, we recommend strengthening the Part 2 / General Offences section to simply ban the worst offences.*
3) Give the AI & Data Commissioner power to regulate, but add parliamentary oversight	*In the current wording, meaningful regulations must be approved by cabinet, which politicises the process and makes it far slower and removed from the expertise on the ground. We initially recommended creating an independent AI Commission (modelled after the CNSC) - if this is too much of a change to the bill, then the AIDC should have these powers. Secondly, the risks of conflict of interest with ISED's mandate to boost innovation are too high to have the Industry Minister and their chosen AIDC perform this work without oversight. We recommend either adding an oversight office based in parliament, and/or ensuring that an independent Minister of AI be assigned.*
4) Make the list of regulated AI value chain entities future-proof by adding a schedule	*In a rapidly evolving sector, regulators will need the flexibility to update the list of which entities in the AI value chain need to be regulated and how (e.g. to include AI hardware). Better to list the entities in a Schedule than in the text of the law, and to allow separate regulations for each. Ideally the current 3 (model developers, those making systems available, and operators) would be removed from the text and included in the Schedule, but the Schedule could instead be used for adding new entities only.*
5) Clarify who in the accountability framework is legally liable	*The Accountability Frameworks introduced in the amendments are a good start, but identifying the individual who is legally liable is essential. We recommend adopting s.3 & 93 of Quebec's Loi 25 that specifies this is the individual with the highest authority in the organisation, who can delegate responsibility to a person in the accountability framework.*

Recommended wording for the Bill

To illustrate what these recommendations would mean in practice, we provide here a copy of the full text of the Bill that includes the Minister's amendments and highlights the specific wording changes needed for it to meet the needs of Canadians and put Canada in a position of global leadership on AI:

Recommended wording for the AI & Data Act

We will be happy to answer any questions about the rationale for specific wording. If you have any questions, simply email us at contact@aigs.ca.