The Honourable François-Philippe Champagne P.C., M.P.
Minister of Innovation, Science and Industry
Innovation, Science, and Economic Development Canada
C.D. Howe Building
235 Queen St, 4th Floor
Ottawa, ON K1A 0H5
Canada

April 23, 2024

Dear Minister Champagne:

BSA | The Software Alliance appreciates the opportunity to share our views on Canada's proposed Artificial Intelligence and Data Act (AIDA), which is part of Bill C-27, the Digital Charter Implementation Act, 2022.

BSA is the leading advocate for the global software industry.[1] BSA members have a significant presence in Canada, employing thousands of workers across the country. BSA members are at the forefront of developing cutting-edge services — including AI — and their products are used by businesses across every sector of the economy.[2] For example, BSA members provide tools including cloud storage and data processing services, customer relationship management software, human resource management programs, identity management services, cybersecurity services, and collaboration software. BSA members are on the leading edge of providing AI-enabled products and services. As a result, they have unique insights into the technology's tremendous potential to spur digital transformation and the policies that can best support the responsible use of AI.

BSA's views are informed by our experience working with member companies to develop the BSA Framework to Build Trust in AI,[3] a risk management framework we published almost three years ago to help companies mitigate the potential for unintended bias in AI systems. Built on a vast body of research and informed by the experience of leading AI developers, the BSA Framework outlines a lifecycle-based approach for performing impact assessments and highlights corresponding best practices. BSA has testified before the

[1] BSA's members include: Adobe, Alteryx, Asana, Atlassian, Autodesk, Bentley Systems, Box, Cisco, CNC/Mastercam, Databricks, DocuSign, Dropbox, Elastic, Graphisoft, Hubspot, IBM, Informatica, Kyndryl, MathWorks, Microsoft, Okta, Oracle, PagerDuty, Palo Alto Networks, Prokon, Rubrik, Salesforce, SAP, ServiceNow, Shopify Inc., Siemens Industry Software Inc., Splunk, Trend Micro, Trimble Solutions Corporation, TriNet, Twilio, Workday, Zendesk, and Zoom Video Communications, Inc.

[2] *See* BSA | The Software Alliance, Artificial Intelligence in Every Sector, *available at* https://www.bsa.org/files/policy-filings/06132022bsaaieverysector.pdf.

[3] *See* BSA | The Software Alliance, Confronting Bias: BSA's Framework to Build Trust in AI, *available at* https://www.bsa.org/reports/confronting-bias-bsas-framework-to-build-trust-in-ai.

200 Massachusetts Avenue, NW
Suite 310
Washington, DC 20001
P 202-872-5500
W bsa.org

United States Congress and the European Parliament on the Framework and its approach to mitigating AI-related risks.[4]

BSA has also previously shared its policy expertise with the Canadian government, particularly on issues relating to the intersection of copyright and AI. For example, BSA provided input on the Industry, Science, and Economic Development Canada's consultation on copyright and generative AI earlier this year,[5] and it previously testified before the Canadian Parliament on the importance of policies that facilitate the data analytic processes that underpin the development of AI.[6] Our experience on these issues informs our recommendations below.

I. Overview: AIDA Undermines the Government's AI Strategies

The Government has undertaken significant efforts to position Canada as a leader on AI, including being the first country in the world to develop a national AI strategy, becoming one of the founding members of the Global Partnership on AI, and making significant investments in AI research and innovation hubs across Canada. As early as 2017, Prime Minister Trudeau predicted that, "in the years to come," Canada "will see this leadership pay dividends in everything from manufacturing improvements to health-care breakthroughs, to stronger and more sustained economic and job growth."[7] Along with these efforts, the Government has also aimed to be a leader in addressing the adverse impacts of AI while ensuring responsible AI innovation through the establishment of a new regulatory framework.

AIDA seeks to regulate the development and deployment of AI broadly and, if amended, would address a range of issues, including risk management and reporting obligations for general purpose and high-impact AI, the implementation of accountability frameworks, and governmental enforcement powers, which include audits and the imposition of criminal penalties. In your letter to the Chair of the House of Commons' Standing Committee on Industry and Technology, which is currently considering AIDA, you emphasized the importance of the legislation to Canadians' trust in the development of AI systems and the impact on the Canadian economy, noting that failure to act would mean that "Canada would

---

[4] *See, e.g.,* Testimony of Victoria Espinel, Public Hearing on AI & Bias, Special Committee on Artificial Intelligence in a Digital Age, European Parliament, Nov. 30, 2021, *available at* https://www.europarl.europa.eu/cmsdata/244265/AIDA_Verbatim_30_November_2021_EN.pdf; Testimony of Victoria Espinel, The Need for Transparency in Artificial Intelligence, Before the Senate Committee on Commerce, Science, and Transportation Subcommittee on Consumer Protection, Product Safety, and Data Security, *available at* https://www.bsa.org/files/policy-filings/09122023aitestimonyoral.pdf.

[5] *See* https://www.bsa.org/policy-filings/canada-bsa-submission-on-artificial-intelligence-and-copyright-policy.

[6] *See generally* https://www.bsa.org/news-events/events/testimony-before-canadian-standing-committee-on-industry-science-and-technology. BSA has also provided comments in response to consultations on Canada's possible accession to the Digital Economy Partnership Agreement, https://www.bsa.org/policy-filings/canada-bsa-comments-on-canadas-accession-to-the-digital-economy-partnership-agreement, and the Office of the Privacy Commissioner's consideration of consent requirements for the transfer of personal information, https://www.bsa.org/policy-filings/canada-bsa-comments-on-the-opcs-consultation-on-consent-requirement-to-transfer-personal-information-for-processing-purposes.

[7] *See* Trudeau Looks to Make Canada "World Leader" in AI Research, phys.org, (March 30, 2017), *available at* https://phys.org/news/2017-03-trudeau-canada-world-leader-ai.html.

200 Massachusetts Avenue, NW
Suite 310
Washington, DC 20001
P 202-872-5500
W bsa.org

not be an attractive location for investors, and Canadians would not reap the full benefits that AI can bring to our innovation, productivity, and competitiveness agenda."[8]

We agree with the important goals that you articulated, but caution that some of the Government's proposed amendments would undermine these objectives. Notably, some of AIDA's obligations are more onerous than other policies around the globe, which makes it more difficult to develop and use AI products and services in Canada.[9] We highlight below potential improvements to the legislation that would address these issues and better achieve the dual aims of spurring innovation and ensuring trustworthy AI.

Specifically, we recommend:

- Narrowing the activities that are classified as "high-impact";
- Defining the roles in the AI value chain;
- Limiting the scope and obligations associated with general purpose AI systems;
- Applying AIDA prospectively;
- Limiting the application of third-party conformity assessments; and
- Removing criminal penalties for violations of AIDA.

I. AIDA's Broad Approach and Criminal Enforcement Regime Departs from International Norms

The Government has indicated that AIDA's interoperability "with legal frameworks in other jurisdictions" is a "key consideration" for facilitating "Canadian companies' access to international markets."[10] However, AIDA's breadth and criminal enforcement regime diverge from other international approaches to addressing the policy implications of AI, including legislation that the EU is expected to adopt next month. The EU struggled to strike the right balance and adopt workable AI policy solutions, and forthcoming guidance and regulations may highlight some of the practical implementation challenges of the EU's approach. In key respects, the Government's proposed amendments to AIDA may pose even greater challenges.

In particular, AIDA, if amended, would depart from international norms in five key ways: (1) AIDA's approach to high-impact AI and general purpose AI systems regulates low-risk uses of AI and imposes more onerous obligations than anywhere else in the world; (2) AIDA does not define the roles in the AI value chain; (3) AIDA applies retroactively; (4) AIDA requires third-party conformity assessments for general purpose AI systems; and, as noted above, (5) AIDA imposes criminal liability, departing from the legislative approach in the EU, voluntary AI governance approaches in the United Kingdom and Singapore, and AI legislative proposals in the United States.

---

[8] *See* Letter from Minister François-Philippe Champagne, P.C., M.P. to Chair Joël Lightbound, M.P., Nov. 28, 2023, *available at* https://www.ourcommons.ca/content/Committee/441/INDU/WebDoc/WD12751351/12751351/MinisterOfInnovationScienceAndIndustry-2023-11-28-Combined-e.pdf.

[9] Throughout the letter, our references to AIDA are to the introduced bill if amended with the Government's proposed edits submitted to Parliament last year.

[10] *See* https://ised-isde.canada.ca/site/innovation-better-canada/en/artificial-intelligence-and-data-act-aida-companion-document.

A. High-Impact AI

Policymakers around the globe have been coalescing around the need to address high-risk uses of AI. AIDA adopts a similar approach in principle, primarily governing "high-impact AI," but its broad classification of activities that constitute high-impact AI applies to low-risk uses and exceeds the scope of high-risk activities governed elsewhere. For example, high-impact AI activities under the Government's proposed schedule for AIDA include the moderation and prioritization of content on online platforms, but this does not pertain to a significant decision that determines individuals' eligibility for critical services, which is the area that poses the most risk to individuals.

Notably, the EU AI Act limits high-risk uses to those that pose a significant risk of harm to health, safety, or fundamental rights. However, AIDA does not contain a similar limitation.[11] In addition, the EU AI Act contains exceptions to the list of high-risk uses, including for AI systems intended to perform a narrow procedural task or intended to complete a previously completed human activity. AIDA does not contain similar exceptions. As a result, the categories of covered activities regulated under AIDA are more expansive than those in the EU AI Act, which impedes global interoperability and imposes unreasonable burdens on low-risk AI.

We understand that the Government intends to further refine issues related to high-impact AI through implementing regulations, but legislation that has a nebulous scope nonetheless poses serious challenges for predictability and clarity, leaving companies uncertain as to how they should adapt their business operations to comply with the law. The law should be clear that it does not authorize the Government to establish rules that impose burdensome obligations on low-risk AI.

B. Defining Roles in the AI Value Chain

Proposals for AI regulatory frameworks around the world define the roles that exist in the AI ecosystem and assign obligations based on those roles. These roles include "developers," who design, create, or produce AI systems, and "deployers," who use the AI systems and interact directly with end users, as well as other parties that integrate AI services into their products along the value chain. Accountability should be assigned to the most appropriate role based on knowledge, control, and position in the AI value chain. This approach will promote more effective risk management and recognizes the different types of information each organization has access to and its ability to implement different risk mitigation measures. Clearly defining the entities in the AI value chain, and allocating obligations to each based on their role, is the cornerstone of a clear and strong regulatory framework that establishes accountability throughout the value chain. We appreciate that the Government's proposed amendments made progress in this area by restructuring AIDA's core requirements to allocate obligations to specific entities, but more work should be done to define those concepts.

To ensure obligations are clearly and appropriately allocated throughout the AI value chain, we strongly recommend that AIDA define these distinct roles. For example, the EU AI Act defines the roles of "provider" and "deployer," and allocates high-risk requirements to each

[11] Although the Government has indicated that AIDA focuses on systems with the "greatest impact on health, safety, and human rights," the text of the Government's proposed amendments does not achieve this objective. *See* https://www.pm.gc.ca/en/news/news-releases/2024/04/07/securing-canadas-ai.

based on their role. Without defining the relevant roles, there is a risk that AIDA will lack clarity regarding who is accountable for what, undermining the law's overall effectiveness.

C. General Purpose AI Systems

The Government's proposed amendments to AIDA relating to general purpose AI systems create similar challenges. They define general purpose AI systems to include systems that can be adapted for many purposes and activities and impose several obligations on them, including those that relate to data use, risk mitigation, human oversight, transparency, and third-party assessments.

Conversely, the EU AI Act defines a general purpose AI system as a system which is based on a general purpose AI model that has the capability to serve a variety of purposes, and it separately defines a general purpose AI model to include an AI model "trained with a large amount of data using self-supervision at scale, that displays significant generality and is capable of competently performing a wide range of distinct tasks."[12] The EU AI Act limits obligations of general purpose AI systems to transparency requirements and technical cooperation, and it limits obligations of general purpose AI models to technical documentation, sharing of information necessary for deploying the model, and compliance with copyright laws. The EU AI Act also imposes some additional obligations on a category of general purpose AI models that pose systemic risks, including model evaluation, assessment and mitigation of risks, serious incident reporting, and cybersecurity protection.

AIDA's approach is broader in scope, as its definition of general purpose AI systems is not based on an underlying general purpose model and covers more low-risk uses of AI than the EU AI Act. In addition, the associated obligations exceed those that apply to the non-systemic risk general purpose AI models under the EU AI Act. Because general purpose AI systems can be widely adapted for different uses, many of these obligations are impractical. For example, the Government's proposed amendments require companies to assess the risks of foreseeable uses of general purpose systems. However, it may be impossible to perform a comprehensive analysis of these use-based considerations for a general purpose AI model developer if it cannot predict the myriad ways in which its technology will be integrated into other systems or deployed in the marketplace. Similarly, in addition to the concerns outlined in Section E below, third-party audits would not ensure an improved risk mitigation, considering the breadth of applications for general purpose AI systems and models, and would likely create significant compliance burdens, without corresponding gains from a risk management perspective.

We recommend narrowing the proposed scope of a general purpose AI system covered by AIDA and defining it as a general purpose model that is "trained with a large amount of data using self-supervision at scale, that displays significant generality and is capable of competently performing a wide range of distinct tasks." We also recommend limiting the related obligations placed on general purpose systems to transparency and information sharing requirements.

D. Retroactive Application

AIDA applies retroactively to all AI systems. Unlike AIDA, the EU AI Act applies prospectively except under limited circumstances, including where a significant change has been made to a high-risk system and for general purpose AI models. AIDA contains several

[12] A draft of the latest publicly available text of the EU AI Act is available here: https://www.europarl.europa.eu/doceo/document/TA-9-2024-0138-FNL-COR01_EN.pdf.

new obligations, which would be difficult to implement in all AI systems currently on the market. Like the EU AI Act, we recommend that AIDA primarily apply prospectively, with an exception for high-impact AI systems that have been substantially modified. In doing so, Canada can ease compliance obligations for companies operating in Canada, including small businesses, establish more parity with international regulatory approaches, and ensure that new obligations apply to the most appropriate category of high-impact AI systems.

E. Third-Party Conformity Assessments

AIDA, if amended as proposed, would require that a third-party conformity assessment be performed for any general purpose AI system. Conversely, the EU AI Act primarily relies on self-assessment, limiting third-party conformity assessments to specific circumstances, such as biometric information. The proposed amendments to AIDA depart from the risk-based approach, applying this onerous and invasive obligation to all general purpose systems without consideration of any heightened risks to individuals.

Moreover, the process of developing auditable standards for AI is nascent. There are few existing procedures or best practices for companies to either: (1) choose a reputable company capable of auditing an AI system, or (2) determine what standards any such auditing company should apply. Indeed, although the International Organization for Standardization has issued some AI-related standards, including guidance on risk management practices, several other standards are still under development.[13] Without common standards, the quality of any audits will vary significantly because different audits may measure against different benchmarks, undermining the goal of obtaining an evaluation based on an objective benchmark. Further, no standards exist today that govern auditing itself. As is the case in regulated industries like accounting and financial services, professional standards and guidelines for auditing are crucial to a well-functioning and mature audit ecosystem. As a result, third-party conformity assessments are not currently an appropriate AI accountability policy solution. Instead, companies' implementation of internal risk mitigation measures is sufficient to address any concerns. We recommend not including a third-party conformity assessment requirement in AIDA.

F. Criminal Penalties

AIDA also departs from international approaches to AI by imposing criminal penalties for violations of the law. By comparison, the EU AI Act imposes administrative fines but does not impose criminal penalties, and other jurisdictions considering AI legislation, including federal and state legislatures in the United States, only impose civil liability. Notably, other countries, such as Singapore, have adopted voluntary approaches to AI governance altogether.[14] Criminal penalties are inappropriate here. AIDA also authorizes administrative monetary penalties, which is sufficient to deter illegal conduct. We understand the Government's interest in maintaining federal jurisdiction over these issues, but imposing criminal liability is not necessary to achieve this objective; AIDA's application to "international and interprovincial trade and commerce" also achieves this result. In short, the imposition of criminal liability is an excessive remedy and diverges significantly from

[13] *See* https://www.iso.org/committee/6794475/x/catalogue/.

[14] *See* Model Artificial Intelligence Governance Framework, Second Edition, *available at* https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Resource-for-Organisation/AI/SGModelAIGovFramework2.pdf.

200 Massachusetts Avenue, NW
Suite 310
Washington, DC 20001
P 202-872-5500
W bsa.org

other global AI policy approaches. Accordingly, we recommend that the provision authorizing criminal penalties in AIDA be removed.

II. AIDA Chills AI Innovation and Adoption in Canada

AIDA's departure from other international AI policy approaches will make it more difficult for companies to operate in Canada, chill AI innovation in Canada, and limit Canadian companies' competitiveness in global markets. The regulation of low-risk AI and imposition of burdensome compliance obligations on general purpose AI systems, the increased compliance challenges resulting from AIDA's retroactive application and the proposed third-party conformity assessment requirements, and the imposition of criminal liability would impede both the development of AI services and Canadian businesses' adoption of those services.

We note that the lack of consultation on the proposed amendments to AIDA has limited industry's opportunity to provide meaningful input on the practical implementation challenges and economic consequences of the proposed approach. The development of AI policies without consideration of industry perspectives has resulted in proposals that both hamper AI innovation and affect growth and productivity of companies across a variety of sectors.

Indeed, AIDA's impact on AI development and adoption limits companies' digital transformation and Canadian economic growth. IBM's Global AI Adoption Index indicated that 42% of enterprise-scale companies surveyed actively use AI in their businesses, and 59% of these companies intend to accelerate their investment in the technology.[15] These businesses are deriving numerous benefits from the adoption of AI, including automation of key business processes, enhanced security and threat detection, and improved customer care.[16] Notably, the index shows that Canadian companies using AI were least likely to accelerate their investment in the past two years.[17] The index also showed that upskilling the workforce was among both the top barriers to AI deployment and top areas of investment.[18]

In recognition of AI's power to enhance the competitiveness of Canadian businesses, Prime Minister Trudeau included $2.4 billion in AI investments in his Budget 2024, which was tabled in Parliament last week, noting that it was "a major investment in our future, in the future of workers, in making sure that every industry, and every generation, has the tools to succeed and prosper in the economy of tomorrow."[19] However, the future decline in AI development and business adoption caused by AIDA's overbroad approach and criminal enforcement scheme will inevitably stymie private sector investment in both the research and development of AI technologies and the preparation of an AI-ready Canadian workforce. As a result, Canadian companies will be unable to leverage the full benefits of AI, thereby undermining the Government's economic initiatives and making Canada less competitive than other countries with policies that spur AI innovation.

---

[15] *See* IBM Global AI Adoption Index, *available at* https://newsroom.ibm.com/2024-01-10-Data-Suggests-Growth-in-Enterprise-Adoption-of-AI-is-Due-to-Widespread-Deployment-by-Early-Adopters.

[16] *Id.*

[17] *Id.*

[18] *Id.*

[19] https://www.pm.gc.ca/en/news/news-releases/2024/04/07/securing-canadas-ai.

Such a result thwarts the important goals that you identified for AIDA. We look forward to serving as a resource to help you achieve your objective of ensuring that AIDA promotes both trustworthiness and AI innovation in Canada.

Sincerely,

Shaundra Watson

Shaundra Watson
Senior Director, Policy
BSA | The Software Alliance

200 Massachusetts Avenue, NW
Suite 310
Washington, DC 20001

P 202-872-5500
W bsa.org