Cassels

Be (Artificially) Intelligent – Examining New Guidance for the Artificial Intelligence and Data Act

March 29, 2023

Artificial intelligence (AI) has resurfaced in the public consciousness since the public release of OpenAI's ChatGPT in late November 2022. While the viral AI language generation model represents the latest frontier of machine learning, the advancement and implementation of AI technology has always been ongoing. From job screening to medical diagnoses to autonomous vehicles, AI technology has formed a silent but integral part of our daily lives.

However, the wide-ranging types and applications of AI have raised serious questions about public safety, spurred by regular occurrences of data and privacy breaches. Just last week, OpenAI announced that a bug exposed personal data from 1.2% of ChatGPT Plus subscribers, allowing some users to see another active user's first and last name, email address, payment address, the last four digits of a credit card number, and credit card expiration date.[1]

The potential of AI is limitless, but the realization of this potential must be appropriately balanced with the protection of individuals and their interests from serious harm. As AI technology rapidly evolves, so too must the laws that regulate AI. How, then, has Canada approached the regulation of AI, and will it be enough?

The Artificial Intelligence and Data Act (AIDA)

In June 2022, the federal government introduced the *Digital Charter Implementation Act, 2022* (Bill C-27) in the House of Commons. (For commentary on Bill C-27 as a whole, please see our article found here.) As part of the bill, the government sought to enact the *Artificial Intelligence and Data Act* (AIDA). The goal of AIDA is to regulate "international and interprovincial trade and commerce in artificial intelligence systems" and prohibit certain conduct that could result in serious harm to individuals and their interests.[2]

Recently, on March 13, 2023, the Canadian government published a companion document to AIDA.[3] The document provides more insight into the timeline of AIDA's implementation, and the framework proposed in AIDA. Below are the key takeaways from the companion document.

Timeline of AIDA

AIDA, as part of Bill C-27, is currently in its second reading in the House of Commons. If and when Bill C-27

receives Royal Assent, consultation on the initial set of AIDA regulations will then commence. The government has proposed a development process for the initial set of AIDA regulations that will consist of two rounds of consultation before and after the development of draft regulations. The process will take at least two years after Bill C-27 receives Royal Assent, which means the first AIDA regulations will not likely come into force any sooner than 2025.

Furthermore, once the first set of AIDA regulations comes into force, the focus of AIDA in the "initial years" will be "on education, establishing guidelines, and helping businesses to come into compliance through voluntary means."[4] The government's intent is to "allow ample time for the ecosystem to adjust to the new framework before enforcement actions are undertaken."[5] However, it is currently unclear as to how long this transition period will be.

Framework of AIDA

The proposed approach under AIDA focuses on three goals:

- Protection of public interest, particularly with respect to safety and human rights, through identifying and regulating high-impact AI systems;
- Ongoing administration, and enforcement of AIDA, through the creation of an office headed by a new AI and Data Commissioner as a centre of expertise in regulation development and administration; and
- Prohibition of reckless and malicious uses of AI, through the introduction of new criminal law provisions.

High-Impact AI Systems

Identification

AIDA focuses on AI systems that would fall under the classification of "high-impact". As such, the criteria for the identification of high-impact AI systems are crucial under AIDA. The companion document captures a number of key factors that the government will consider in determining which AI systems would be considered to be high-impact, including:

- Evidence of risks of harm to health and safety or of adverse impact on human rights, based on both the intended purpose and potential unintended consequences of the AI system;
- Severity of potential harms;
- Scale of use;
- Nature of harms and adverse impacts that have already taken place;

- Extent to which opt-out from the AI system, for practical and legal reasons, is not reasonably possible;
- Imbalances of economic or social circumstances or age of impacted persons; and
- Degree to which risks are adequately regulated under another law.

As an illustrative list, the companion document identified the following as "examples of systems that are of interest to the Government in terms of their potential impacts."[6]

- Screening systems impacting access to services or employment, as they have the potential to produce discriminatory outcomes and economic harm against women and other marginalized groups;
- Biometric systems used for identification and inference, as they may have significant impacts on mental health and autonomy;
- Systems that can influence human behaviour at scale, as they may negatively affect psychological and physical health; and
- Systems critical to health and safety, such as data from sensors, as these systems may cause direct physical harm or lead to biased outcomes.

Obligations

Once an AI system is classified as high-impact, it must satisfy a number of regulatory requirements before it can be made available for use.

The principles that will guide the development of the AIDA regulations for high-impact AI systems are:

1. **Human oversight**: design and development of high-impact AI systems to allow humans managing the system's operations to exercise meaningful oversight, which is assessed contextually.
2. **Monitoring**: measurement and assessment of high-impact AI systems and their outputs to support effective human oversight.
3. **Transparency**: publication of information to allow public to understand the capabilities, limitations, and potential impacts of the high-impact AI systems.
4. **Fairness and equity**: awareness of the potential for, and mitigation of, discriminatory outcomes.
5. **Safety**: proactive assessment of high-impact AI systems to identify and to mitigate potential harms, including through reasonably foreseeable misuse.
6. **Accountability**: implementation of governance mechanisms to ensure legal compliance.
7. **Validity**: consistent performance with intended objectives.
8. **Robustness**: stability and resilience of high-impact AI systems in a variety of circumstances.

According to the companion document, obligations on businesses contributing to or interacting with a high impact AI system may have different obligations, in proportion to the associated risks. For example, a

business that designs or develops a high-impact AI system will have different obligations from a business that either makes the high-impact AI system available for use or manages the operations of the AI system. The government has taken the position that research and development of methodologies are not, on their own, to be regulated under AIDA.

Oversight and Enforcement

The administration and enforcement of AIDA is divided between administrative offences, regulatory offences, and true criminal offences. The former will be the responsibility of the Minister of Innovation, Science, and Industry (the Minister), with the support of the new AI and Data Commissioner and their office. The latter two will be the responsibility of the Public Prosecution Service of Canada (PPSC), and the Minister will only have the ability to refer cases to the PPSC but no role in determining who should be prosecuted.

Administrative Offences

The Minister's investigative powers include ordering the production of records to demonstrate compliance with AIDA and ordering an independent audit. Where there is a risk of imminent harm, the Minister can also order the cessation of use of a system and publicly disclose information regarding contraventions of AIDA or for the purpose of preventing harm.

The remedy available to the Minister for such offences is administrative monetary penalties (AMPs). While AIDA allows for the creation of an AMPs regime, the details of the regime will emerge following consultations.

Regulatory Offences

To prosecute a regulatory offence, the PPSC must determine that a prosecution is in the public interest. The standard of proof for these regulatory offences is guilt proven beyond a reasonable doubt. A full defence available to a business charged with a regulatory offence is to show that it had taken due care in complying with its obligations.

True Criminal Offences

Where a party engages in knowing and intentional behaviour that causes serious harm with an AI system, the PPSC can prosecute them for a true criminal offence. These criminal offences relate to the creation of new criminal law provisions, as further explained below.

New Criminal Law Provisions

The third and final goal of AIDA's framework is the prohibition of reckless and malicious uses of AI that cause serious harm to Canadians and their interests. AIDA would create three new criminal offences related to AI systems:

1. Knowingly possessing or using unlawfully obtained personal information to design, develop, use, or make available for use in an AI system. An illustrative example is the knowing use of personal information obtained from a data breach to train an AI system.
2. Making an AI system available for use, knowing, or being reckless as to whether, it is likely to cause serious harm or substantial damage to property, where its use actually causes such harm or damage.
3. Making an AI system available for use with intent to defraud the public and to cause substantial economic loss to an individual, where its use actually causes such harm or damage.

Conclusion

AIDA attempts to balance the competing interests in the proliferation of AI, as it is "designed to protect individuals and communities from the adverse impacts associated with high-impact AI systems [while supporting] the responsible development and adoption of AI across the Canadian economy."[7] AIDA also attempts to align with the current regulatory approaches of other international jurisdictions and organizations, such as the EU's AI Act, the Organization of Economic Co-operation and Development (OECD) AI Principles, and the US National Institute of Standards and Technology (NIST) Risk Management Framework.

As AIDA continues to develop through parliamentary debates and public consultations, Canada's first regulatory framework for AI will likely become more concrete, including the legal obligations for businesses interacting with AI systems to examine and fulfill.

Furthermore, while AIDA is aimed at mitigating the risks of high-impact AI systems, it does not address many other legal considerations associated with artificial intelligence, such as copyright law. As such, AIDA is likely the first of several AI-focused laws or provisions to be introduced in the coming years.

Businesses contemplating the current and future requirements of their AI systems are encouraged to contact our Information Technology & Data Privacy Group for assistance with navigating the evolving regulatory process.

Cassels

[1] OpenAI, “March 20 ChatGPT outage: Here’s what happened” (24 March 2023), online: https://openai.com/blog/march-20-chatgpt-outage

[2] 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*, 1st Sess, 44th Parl, 2022 (first reading 16 June 2022) [“Bill C-27”] at Part 3, cl 4.

[3] Innovation, Science and Economic Development Canada, “The *Artificial Intelligence and Data Act* (*AIDA*) – Companion document” (13 March 2023), online: https://ised-isde.canada.ca/site/innovation-better-canada/en/artificial-intelligence-and-data-act-aida-companion-document.

[4] Ibid.

[5] Ibid.

[6] Ibid.

[7] Ibid.

This publication is a general summary of the law. It does not replace legal advice tailored to your specific circumstances.