

BULLETIN

The Regulation of Artificial Intelligence in Canada and Abroad: Comparing the Proposed AIDA and EU AI Act

READING TIME
17 MINUTE READ

OCTOBER 18, 2022

Privacy & Cybersecurity Bulletin

Laws governing technology have historically focused on the regulation of information privacy and digital communications. However, governments and regulators around the globe have increasingly turned their attention to artificial intelligence (AI) systems. As the use of AI becomes more widespread and changes

how business is done across industries, there are signs that existing declarations of principles and ethical frameworks for AI may soon be followed by binding legal frameworks. [\[1\]](#)

On June 16, 2022, the Canadian government tabled Bill C-27, the [**Digital Charter Implementation Act, 2022**](#) [↗](#). Bill C-27 proposes to enact, among other things, the *Artificial Intelligence and Data Act* (AIDA). Although there have been previous efforts to regulate automated decision-making as part of federal privacy reform efforts, AIDA is Canada's first effort to regulate AI systems outside of privacy legislation. [\[2\]](#)

If passed, AIDA would regulate the design, development, and use of AI systems in the private sector in connection with interprovincial and international trade, with a focus on mitigating the risks of harm and bias in the use of “high-impact” AI systems. AIDA sets out positive requirements for AI systems as well as monetary penalties and new criminal offences on certain unlawful or fraudulent conduct in respect of AI systems.

▼ Comparing AIDA and the EU AI Act

Prior to AIDA, in April 2021, the European Commission presented a draft legal framework for regulating AI, the [**Artificial Intelligence Act**](#) [↗](#) (EU AI Act), which was one of the first attempts to comprehensively regulate AI. The EU AI Act sets out harmonized rules for the development, marketing, and use of AI and imposes risk-based requirements for AI systems and their operators, as well as prohibitions on certain harmful AI practices.

Broadly speaking, AIDA and the EU AI Act are both focused on mitigating the risks of bias and harms caused by AI in a manner that tries to be balanced with the need to allow technological innovation. In an effort to be “future-proof” and keep pace with advances in AI, both AIDA and the EU AI Act define “artificial intelligence” in a technology-neutral manner. However, AIDA relies on a more principles-based approach, while the EU AI Act is more prescriptive in classifying “high-risk” AI systems and harmful AI practices and controlling their development and deployment. Further, much of the substance and details of AIDA are left to be elaborated in future regulations, including the key definition of “high risk” AI systems to which most of AIDA's obligations attach.

The table below sets out some of the key similarities and differences between the current drafts of AIDA and the EU AI Act.

Key Definitions	
AIDA	EU AI Act
<p>“Artificial intelligence system” means a technological system that, autonomously or partly autonomously, processes data related to human activities through the use of a genetic algorithm, a neural network, machine learning or another technique in order to generate content or make decisions, recommendations or predictions.</p>	<p>“Artificial intelligence system” means software that is developed with one or more techniques and approaches specified in the legislation (e.g., machine learning approaches, logic and knowledge-based approaches and statistical approaches) and which can, for a given set of human-defined objectives, generate outputs such as content, predictions, recommendations, or decisions influencing the environments they interact with.</p>
<p>“High-impact system” means an artificial intelligence system that meets the criteria established in future regulations.</p>	<p>“High-risk system” means:</p> <ul style="list-style-type: none"> the AI system is intended to be used as a safety component of a specified regulated product, or is itself a specified regulated product (e.g., machinery, toys or radio equipment), that is subject to regulatory approvals before being placed on the market; or specified AI systems which pose a high risk of harm to health and safety or the fundamental rights of persons (e.g., systems for biometric identification and the management

	and operation of critical infrastructure).
<p>“Harm” means (a) physical or psychological harm to an individual; (b) damage to an individual’s property; or (c) economic loss to an individual.</p>	<p>“Serious incident” means any incident that directly or indirectly leads, might have led or might lead to:</p> <ul style="list-style-type: none"> • the death of a person or serious damage to a person’s health, to property or the environment; or • a serious and irreversible disruption of the management and operation of critical infrastructure.
<p>Application</p>	
<p>AIDA</p>	<p>EU AI Act</p>
<p>AIDA applies to “persons” (including trusts, joint ventures, partnerships, unincorporated associations, and any other legal entities) who carry out any of the following “regulated activities” in the course of international or interprovincial trade and commerce:</p> <ul style="list-style-type: none"> • processing or making available for use of any data relating to human activities for the purpose of designing, developing or using an AI system; and • designing, developing or making available for use an AI system or managing its operations. 	<p>The EU AI Act applies to:</p> <ul style="list-style-type: none"> • “Providers” (including a natural or legal person, public authority, agency, or other body) of AI systems who place on the market or put into service such systems, irrespective of whether those providers are established within the EU or in a third country; • Users of AI systems located in the EU; and • Providers and users of AI systems located outside the EU, where the output produced by those systems is used in the EU. <p>The EU AI Act applies irrespective of whether the AI system is free or for</p>

	<p>payment (although the AI system must be put into service in the course of commercial activity).</p>
<p>AIDA does <u>not</u> apply to:</p> <ul style="list-style-type: none"> • government institutions as defined in section 3 of the <i>Privacy Act</i>; and • products, services or activities that are under the direction or control of specified federal security agencies, such as the Minister of National Defence and the Director of the Canadian Security Intelligence Service. 	<p>The EU AI Act does <u>not</u> apply to:</p> <ul style="list-style-type: none"> • AI systems developed or used exclusively for military purposes; and • foreign public authorities or international organizations who use AI systems in the framework of international agreements for law enforcement and judicial cooperation with the EU or EU Member States.

Prohibitions

AIDA	EU AI Act
<p>AIDA does not stipulate an outright ban on AI systems presenting an unacceptable level of risk.</p> <p>It does, however, make it an offence to:</p> <ul style="list-style-type: none"> • possess or use personal information for the purpose of creating an AI system if the personal information was not lawfully obtained; • knowingly (or with reckless disregard) use an AI system that is likely to cause serious physical or psychological harm to an individual or substantial damage to property, if such harm occurs; or • make an AI system available for use with the intent to defraud the public 	<p>The EU AI Act prohibits certain AI practices and certain types of AI systems, including:</p> <ul style="list-style-type: none"> • systems aimed at distorting a person’s behaviour that are likely to cause physical or psychological harm to an individual by using subliminally manipulative techniques or techniques exploitive of individual vulnerabilities based on their age, physical or mental incapacities; • social scoring systems used by public authorities, or on their behalf, that lead to unjustified, disproportionate or unrelated

and to cause substantial economic loss to an individual, if such loss occurs.	<p>detrimental or unfavourable treatment of certain persons or groups; and</p> <ul style="list-style-type: none"> the use of AI systems for “real-time” biometric identification of individuals in publicly accessible spaces for law enforcement purposes. <u>[3]</u>
---	---

Use of Data

AIDA	EU AI Act
<p>Persons who process anonymized data for use in AI systems must establish measures (in accordance with future regulations) with respect to:</p> <ul style="list-style-type: none"> the manner in which data is anonymized; and the use or management of anonymized data. 	<p>High-risk systems that use data sets for training, validation and testing must be subject to appropriate data governance and management practices that address:</p> <ul style="list-style-type: none"> design choices, data collection and data preparation; the formulation of assumptions; assessments of the availability of data; and an examination of possible biases and the identification of any possible data gaps or shortcomings. <p>Data sets must:</p> <ul style="list-style-type: none"> be relevant, free of errors and complete; account for the characteristics or elements of the specific geographical, behavioural or functional setting within which the

	<p>AI system is intended to be used; and</p> <ul style="list-style-type: none"> only include special categories of personal data if appropriate safeguards are in place.
<p>Requirements for AI Systems</p>	
<p>AIDA</p>	<p>EU AI Act</p>
<p>Assessment. Persons responsible for an AI system must assess (in accordance with future regulations) whether it is a “high-impact system.”</p>	<p>Assessment. The EU AI Act takes a graduated approach:</p> <ul style="list-style-type: none"> AI systems with “unacceptable risk” are prohibited; AI systems with “high risk” are permitted, subject to a conformity assessment and compliance requirements, including a certification scheme; AI systems with “transparency risks” are permitted, subject to transparency obligations; and AI systems with “minimal or no risk” are permitted with no restrictions.
<p>Risk management. Persons responsible for “high-impact systems” must:</p> <ul style="list-style-type: none"> establish measures (in accordance with future regulations) to identify, assess, and mitigate the risks of harm or biased output that could result from the use of the system; and 	<p>Risk management. High-risk systems must:</p> <ul style="list-style-type: none"> undergo a conformity assessment procedure and be registered with a “declaration of conformity” before being put into use; have a risk management system to identify and evaluate risks through the system’s lifecycle;

- establish measures (in accordance with future regulations) to monitor compliance with such mitigation measures.

- have automatic event logging capabilities;
- be sufficiently transparent to allow users to interpret the system's output and use it appropriately;
- be accompanied by concise and clear instructions for use that includes the relevant information set out in the EU AI Act;
- allow for effective human oversight to prevent or minimize risks to health, safety or fundamental rights; and
- achieve an appropriate level of robustness and cybersecurity.

Transparency. Persons responsible for “high-impact systems” must publish on a public website a plain-language description of the AI system which explains:

- how the system is intended to be used;
- the types of content it is intended to generate and the decisions, recommendations or predictions that it is intended to make;
- the mitigation measures established in respect of the system; and
- any other information required by future regulations.

Transparency. AI systems which interact with individuals and pose transparency risks, such as those that incorporate emotion recognition systems or risks of impersonation or deception, are subject to additional transparency obligations.

Regardless of whether or not the system qualifies as high-risk, individuals must be notified that they are:

- interacting with an AI system, unless this is obvious from the circumstances and context of use; and
- exposed to an emotion recognition system, a biometric categorisation system, or a “deep fake” (i.e., AI

	generated or manipulated image, audio or video content).
Record-Keeping & Reporting Requirements	
AIDA	EU AI Act
<p>Persons responsible for AI systems must keep records (in accordance with future regulations) describing:</p> <ul style="list-style-type: none"> • measures they have established to identify, assess and mitigate the risks of harm or biased output that could result from the use of the AI system; and • reasons to support their assessment of whether or not the AI system is a “high-impact system”. 	<p>High-risk AI systems must:</p> <ul style="list-style-type: none"> • have technical documentation drawn up before being placed on the market or put into service; such documentation must, amongst other things, demonstrate compliance of the high-risk system with the requirements set out in the EU AI Act; and • be designed and developed in such a way as to enable automatic event logging capabilities while in operation, consistent with recognized standards or common specifications (more prescriptive requirements apply to high-risk systems performing biometric identification and categorisation). <p>Providers of high-risk AI systems must:</p> <ul style="list-style-type: none"> • develop a quality management system to ensure compliance; and • establish a post-market monitoring system to monitor the performance and compliance of high-risk AI systems throughout their lifecycle.

Notification Requirements	
AIDA	EU AI Act
Persons responsible for “high-impact systems” must notify the Minister of Industry if the use of the system results or is likely to result in material harm, as soon as feasible.	Providers of “high-risk” AI systems must report any serious incident or malfunctioning which constitutes a breach of the EU AI Act or of obligations under EU law intended to protect fundamental rights of individuals.
Monitoring Authority & Oversight	
AIDA	EU AI Act

The Minister of Industry may designate an official to be the Artificial Intelligence and Data Commissioner, whose role is to assist in the administration and enforcement of AIDA. The Minister may delegate any of their powers or duties under AIDA to the Commissioner.

The Minister of Industry has the following powers:

- **Public awareness.** Promote public awareness of AIDA and publish recommendations or guidelines with respect to compliance with AIDA.
- **Record collection.** Order the production of records that a person is required to maintain under AIDA (i.e., system assessment, risk management, monitoring measures, and data anonymization).
- **Auditing.** Order an audit with respect to a possible contravention of AIDA and subsequently order corrective or preventive actions pursuant to the audit report's findings.
- **Cessation.** Order that a person responsible for a high-impact system cease using it if there is reason to believe that the system gives rise to a serious risk of imminent harm.

The European Artificial Intelligence Board will assist the European Commission in providing guidance and overseeing the application of the EU AI Act. Each Member State will designate or establish a national supervisory authority.

The Commission has the authority to:

- maintain a publicly accessible database of information concerning high-risk systems;
- oversee the conformity assessment process for high-risk systems; and
- oversee market surveillance activities.

Penalties & Offences

AIDA

EU AI Act

Persons who commit a “violation” of AIDA or its regulations may be subject to **administrative monetary penalties**, the details of which will be established by future regulations. Administrative monetary penalties are intended to promote compliance with AIDA.

Contraventions to AIDA’s governance and transparency requirements can result in **finances**:

- up to the greater of \$10 million and 3% of global revenues, or, when prosecuted as a summary offence, the greater of \$5 million and 2% of global revenues; or
- for individuals, an amount at the discretion of the court, up to a maximum of \$50,000.

Persons who commit more serious **criminal offences** (e.g., contravening the prohibitions noted above or obstructing or providing false or misleading information during an audit or investigation) may be liable to:

- a fine of up to \$25 million or 5% of global revenues; or
- in the case of an individual, a fine at the discretion of the court or imprisonment.

Penalties under the EU AI Act include:

- up to 6% of total global annual turnover, or 30,000 EUR in the case of an individual, for engaging in prohibited practices or failing to meet data governance requirements;
- up to 4% of total global annual turnover, or 20,000 EUR in the case of an individual, for any other violation; and
- additional fines applicable to EU institutions, agencies and bodies.

Each Member State may specify additional penalties for infringements of the EU AI Act.

▼ Key Comparisons Between AIDA and the EU AI Act

▼ Definition of AI

While both acts define AI systems relatively broadly, the definition provided in AIDA is narrower. AIDA only encapsulates technologies that process data autonomously or partly autonomously, whereas the EU AI Act does not stipulate any degree of autonomy. This distinction in AIDA is arguably a welcome divergence from the EU AI Act, which as currently drafted would appear to include even relatively innocuous technology, such as the use of a statistical formula to produce an output. That said, there are indications that the EU AI Act's current definition may be modified before its final version is published, and that it will likely be accompanied by regulatory guidance for further clarity. [\[4\]](#)

▼ Risk Assessment and Management

Both acts are focused on avoiding harm, a concept they define similarly. The EU AI Act is, however, slightly broader in scope as it considers serious disruptions to critical infrastructure a “harm,” whereas AIDA is solely concerned with harm suffered by individuals.

Under AIDA, “high-impact systems” will be defined in future regulations, so it is not yet possible to compare AIDA's definition of “high-impact systems” to the EU AI Act's definition of “high-risk systems”. The EU AI Act identifies two categories of “high-risk systems”. The first category is AI systems intended to be used as safety components of products, or as products themselves. The second category is AI systems listed in an annex to the act and which present a risk to the health, safety, or fundamental rights of individuals. It remains to be seen how Canada would define “high-impact systems”, but the EU AI Act provides an indication of the direction the federal government could take.

Similarly, AIDA also defers to future regulations with respect to risk assessments, while the proposed EU AI Act sets out a graduated approach to risk in the body of the act. Under the EU AI Act, systems presenting an unacceptable level of risk are banned outright. In particular, the EU AI Act explicitly bans manipulative or exploitive systems that can cause harm, “real-time” biometric identification systems used in public spaces by law

enforcement, and all forms of social scoring. AI systems presenting low or minimal risk are largely exempt from regulations, except for transparency requirements.

AIDA only imposes transparency requirements on high-impact AI systems, and does not stipulate an outright ban on AI systems presenting an unacceptable level of risk. It does, however, empower the Minister of Industry to order that a high-impact system presenting a serious risk of imminent harm cease being used.

▼ Application and Scope


AIDA's application is limited by the constraints of the federal government's jurisdiction. AIDA broadly applies to actors throughout the AI supply chain from design to delivery, but only as their activities relate to international or interprovincial trade and commerce. AIDA does not expressly apply to intra-provincial development and use of AI systems. Government institutions (as defined under the *Privacy Act*) are excluded from AIDA's scope, as are products, services, and activities that are under the direction or control of specified federal security agencies.

The EU AI Act specifically applies to providers (although this may be interpreted broadly) and users of AI systems, *including* government institutions but *excluding* where AI systems are exclusively developed for military purposes. The EU AI Act also expressly applies to providers and users of AI systems insofar as the output produced by those systems is used in the EU.

▼ Data Governance

AIDA is largely silent on requirements with respect to data governance. In its current form, it only imposes requirements on the use of anonymized data in AI systems, most of which will be elaborated in future regulations. AIDA's data governance requirements will apply to anonymized data used in the design, development, or use of any AI system, whereas the EU AI Act's data governance requirements will apply only to high-impact systems.

The EU AI Act sets the bar very high for data governance. It requires that training, validation, and testing datasets be free of errors and complete. In response to criticisms of

this standard for being too strict, the European Parliament has introduced an amendment  to the act that proposes to make “error-free” and “complete” datasets an overall objective to the extent possible, rather than a precise requirement.

▼ Other Key Obligations

While AIDA and the EU AI Act both set out requirements with respect to assessment, monitoring, transparency, and data governance, the EU AI Act imposes a much heavier burden on those responsible for high-risk AI systems. For instance, under AIDA, persons responsible for such systems will be required to implement mitigation, monitoring, and transparency measures. The EU AI Act goes a step further by putting high-risk AI systems through a certification scheme, which requires that the responsible entity conduct a conformity assessment and draw up a “declaration of conformity” before the system is put into use.

Both acts impose record-keeping requirements. Again, the EU AI Act is more prescriptive, but contrary to AIDA, its requirements will only apply to high-risk systems, whereas AIDA’s record-keeping requirements would apply to all AI systems.

Finally, both acts contain notification requirements that are limited to high-impact (AIDA) and high-risk (EU AI Act) systems. AIDA imposes a slightly heavier burden, requiring notification for all uses that are likely to result in material harm. The EU AI Act only requires notification if a serious incident or malfunction has occurred.

▼ Enforcement and Penalties

Both AIDA and the EU AI Act provide for the creation of a new monitoring authority to assist with administration and enforcement. The powers attributed to these entities under both acts are similar.

Both acts contemplate significant penalties for violations of their provisions. AIDA’s penalties for more serious offences – up to \$25 million CAD or 5% of the offender’s gross global revenues from the preceding financial year – are significantly greater than those found in Quebec’s newly revised privacy law and the EU’s General Data Protection Regulation (GDPR). The EU AI Act’s most severe penalty is higher than both the GDPR

and AIDA's most severe penalty: up to €30 million or 6% of gross global revenues from the preceding financial year for non-compliance with prohibited AI practices or the quality requirements set out for high-risk AI systems.

In contrast to the EU AI Act, AIDA also introduces new criminal offences for the most serious offences committed under the act.

Finally, the EU AI Act would also grant discretionary power to Member States to determine additional penalties for infringements of the act.

▼ Takeaways and Next Steps

While both AIDA and the EU AI Act have broad similarities, it is impossible to predict with certainty how similar they could eventually be, given that so much of AIDA would be elaborated in future regulations. Further, at the time of writing, Bill C-27 has only completed first reading, and is likely to be subject to amendments as it makes its way through Parliament.

It is still unclear how much influence the EU AI Act will have on AI regulations globally, including in Canada. Regulators in both Canada and the EU may aim for a certain degree of consistency. Indeed, many have likened the EU AI Act to the GDPR, in that it may set global standards for AI regulation just as the GDPR did for privacy law.

Regardless of the fates of AIDA and the EU AI Act, organizations should start considering how they plan to address a future wave of AI regulation.

For more information on the potential implications of the new Bill C-27, Digital Charter Implementation Act, 2022, please see our bulletin, [The Canadian Government Undertakes a Second Effort at Comprehensive Reform to Federal Privacy Law](#) , on this topic.

[1] There have been a number of recent developments in AI regulation, including the United Kingdom's [Algorithmic Transparency Standard](#), China's draft [regulations](#) on algorithmic recommendation systems in online services, the United States' *Algorithmic Accountability Act of 2022*, and the collaborative effort between Health Canada, the FDA and the United Kingdom's Medicines and Healthcare Products Regulatory Agency to publish [Guiding Principles on Good Machine Learning Practice for Medical Device Development](#).

[2] In the public sphere, the *Directive on Automated Decision-Making* guides the federal government's use of automated decision systems.

[3] This prohibition is subject to three exhaustively listed and narrowly defined exceptions where the use of such AI systems is strictly necessary to achieve a substantial public interest, the importance of which outweighs the risks: (1) the search for potential victims of crime, including missing children; (2) certain threats to the life or physical safety of individuals or a terrorist attack; and (3) the detection, localization, identification or prosecution of perpetrators or suspects of certain particularly reprehensible criminal offences.

[4] As an indication of potential changes, the Slovenian Presidency of the Council of the European Union tabled a [proposed amendment](#) to the act in November 2021 that would effectively narrow the scope of the regulation to machine learning.

▼ Authors

- Christopher Ferguson, Partner, Toronto, ON, +1 416 865 4425, cferguson@fasken.com
- Heather Whiteside, Associate, Toronto, ON, +1 416 865 5476, hwhiteside@fasken.com

The content of this website may contain attorney advertising under the laws of various states.