Canada's Artificial Intelligence and Data Act: Impact for businesses

June 27, 2022

On June 15, 2022, the Minister of Innovation, Science and Industry, François-Phillippe Champagne introduced 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* (or *Digital Charter Implementation Act, 2022*).

The greater part of Bill-27 is the successor to the former Bill C-11, tabled in 2020, reintroducing in modified form the *Consumer Privacy Protection Act* (CPPA) and the *Personal Information and Data Protection Tribunal Act* (PIDPTA).

C-27 also introduces new proposed legislation that is the subject of this bulletin: the *Artificial Intelligence and Data Act* (AIDA). AIDA aims to regulate the development and use of artificial intelligence systems (AI or AI systems) in the private sector.

AIDA, if enacted, would be entirely new legislation in the Canadian context: no provincial or territorial governments have yet tabled bills that seek to regulate private sector development and use of AI. Moreover, among major market jurisdictions, Canada is second only to the European Union in formally introducing such draft legislation for consideration.

What you need to know

- This article provides an overview of the key aspects of AIDA and its impact on Canadian businesses. As more fully detailed herein, this new regime governing AI systems would include the following:
- **A principles-based, as opposed to a rights-based framework:**
    - AIDA is focused on ensuring proper governance and control of AI systems and does not create any new individual rights.
    - AIDA is concerned with preventing (i) physical or psychological harm to an individual, damage to an individual's property, and economic loss to an individual, and (ii) biased output (output of AI systems that adversely differentiates without justification on one or more of the prohibited grounds of discrimination set out in the *Canadian Human Rights Act*).
- **Broad scope:**

- The definition of AI system provided in AIDA is broad, presumably to address the wide range of risks to individual rights that the use of AI systems presents.
- The range of persons obliged to abide by AIDA's requirements is broadly scoped to include designers, developers, providers and managers of AI systems.
- Although not expressly applicable to intra-provincial development and use of AI systems, given the nature of development and use, it seems likely that the federal government intends AIDA to govern substantially all development and use of AI in Canada.

- **Assessment, mitigation and monitoring obligations:**
  - Developers, designers, providers and managers of AI systems will need to undertake assessments to determine whether they are "high-impact".
  - High-impact systems will require mitigation measures and ongoing monitoring for compliance, to be undertaken by designers, developers, providers and managers of AI systems.
- **Transparency:**
  - AIDA creates a nuanced transparency regime for high-impact systems.
  - Persons making AI systems available for use will be required to publish a plain-language explanation of the **intended use** of the AI system, and the decisions, recommendations or predictions that it is intended to make.
  - Persons managing the operations of an AI system (e.g., organizations putting it to use) will be required to publish a plain-language explanation of the **actual use** of the AI system, and the decisions, recommendations or predictions that it makes.
- **Obligations in relation to anonymized data:**
  - Designers, developers, providers and managers of AI systems that use anonymized data and persons that make anonymized data available for the purpose of designing, developing or using an AI system must establish measures with respect to (a) the manner in which the data is anonymized and (b) the use or management of anonymized data.
  - Note that these obligations are general and not limited to high-impact systems.
- **Obligations to report to the Minister:**
  - A person who is responsible for a high-impact system must notify the Minister if the use of the system results or is likely to result in material (a) physical or psychological harm to an individual; (b) damage to an individual's property; or (c) economic loss to an individual.
- **Protections for confidential business information:**
  - Despite stringent transparency requirements for designers and operators and the powers of the Minister to publish information about AI systems, AIDA contains many provisions designed to protect commercial interest in trade secrets.
- **Ministerial powers and enforcement tools:**
  - The Minister may delegate its powers apart from the power to make regulations, and may designate a senior official of the department to be the Artificial Intelligence and Data Commissioner.
  - The Minister or its delegate will have order-making powers that may be enforced as orders of the Federal Court.
  - AIDA proposes to introduce by regulation an administrative monetary penalty scheme, with the potential that the power to apply such penalties

will be granted directly to the newly created Artificial Intelligence and Data Commissioner.
- Fines for most offences under AIDA can go up to a maximum of C$10,000,000, or, if greater, the amount corresponding to 3 per cent of the organization's global gross revenues in its previous fiscal year. Fines for certain offences can climb to a maximum of C$25,000,000, or, if greater, the amount corresponding to 5 per cent of the organization's global gross revenues in its previous fiscal year.
- Provisions that enable the Minister to publish information about AI systems that it believes could give rise to a serious risk of imminent harm.

Introduction

The federal government has indicated that AIDA aims to foster trust in the development and deployment of AI systems, by focusing on governance of "high-impact" systems, establishing a new AI and Data Commissioner to monitor compliance, and providing for criminal penalties where data is obtained unlawfully for AI development or the reckless deployment of AI poses serious harm.

Although it may be inspired to some extent by the EU's 2021 proposal for an *Artificial Intelligence Act* (the EU Proposed AI Regulation),[1] particularly insofar as both take a risk-based approach, it is also unlike the EU Proposed AI Regulation in various respects. For example, the EU Proposed AI Regulation applies to both the public and private sectors, and creates certain exceptions for public sector uses of AI (in particular, law enforcement). AIDA, on the other hand, excludes all Canadian federal government institutions and may be extended to exclude federal or provincial departments or agencies by regulation (AIDA s. 3). In addition, the EU Proposed AI Regulation sets out several specific prohibited AI practices, and sets out criteria for determining whether an AI system presents high, limited or minimal risks. AIDA, by contrast, sets out no specific prohibited practices and appears to contemplate a distinction only between high-risk systems and all other systems.

AIDA is also considerably less elaborate than the EU Proposed AI Regulation, although the relative simplicity may be only apparent: AIDA proposes to leave many salient matters to regulation, which, given the subject matter of the proposed law, may turn out to be quite complex.

Our general impression of AIDA is that it provides a flexible framework, given that many details will be set out in regulations, but also creates significant responsibilities both for developers of AI algorithms and models and for providers of data, which may have an unintended chilling effect on development and innovation. We look forward to the debates, deliberations in committee, and consultations that we expect to commence when Parliament resumes its activities this Fall.

Definition of AI system, the CPPA and the federal Directive on Automated Decision-Making

AIDA defines "artificial intelligence system" as "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" (AIDA s. 2).

This definition is broad, presumably to address the wide range of risks to individual rights that the use of AI systems presents. It risks being overbroad, as the catch-all phrases "another technique" and "generate content" could capture a wide variety of processing systems that intuitively fall outside even generous interpretations of the term "AI".

As we have discussed elsewhere, proposed definitions for artificial intelligence are often unsatisfactory for a variety of reasons. It is difficult to avoid the conclusion that artificial intelligence is an aspirational term that means fundamentally different things to different people, which makes it challenging to produce a practical legal definition. We expect therefore that there will be vigorous discussion of the definition in committee review and parliamentary debates.

AIDA interacts to some degree with the CPPA, owing to the CPPA's treatment of "automated decision systems". This term overlaps with AIDA's definition of "artificial intelligence system", but the two are not coterminous. The CPPA defines "automated decision systems" as "technology that assists or replaces the judgment of human decision-makers through the use of a rules-based system, regression analysis, predictive analytics, machine learning, deep learning, a neural network or other technique" (CPPA s.2).

These differences in scope are not surprising, given that the CPPA seeks to address the accuracy of decisions rendered by automated decision systems that make use of personal information, and AIDA is concerned with the wider risks to individual rights that the use of AI systems presents. We have addressed key interactions between the two proposed laws in our publication on the CPPA and the PIDPTA.

In this connection, it bears mentioning that the CPPA definition for an automated decision system echoes the one given in the federal Directive on Automated Decision-Making that applies to public sector entities (the federal Directive). Like the CPPA, the federal Directive is concerned specifically with technology that assists or replaces the judgement of human decision-makers, but like AIDA, is concerned with a broader set of risks than the CPPA. Because of these overlapping concerns, we think it likely that some aspects of AIDA will be elaborated through regulation or interpretation in ways that align with certain aspects of the federal Directive, as we discuss below.

Scope

AIDA applies to "regulated activity" carried out in the course of international or interprovincial trade and commerce (AIDA s. 5(1)). The language used indicates that the legislation is made pursuant to the federal Parliament's trade and commerce power under section 91(2) of the *Constitution Act, 1867*, suggesting that the federal government intends to leave the provinces to legislate on intraprovincial uses of AI: unlike the CPPA (and its predecessor PIPEDA), AIDA does not clearly apply interprovincially in the absence of provincial law that has been declared substantially similar by regulation (CPPA s. 122(3)). That said, given the relatively narrow circumstances in which an AI system would be developed and deployed solely for use

within a province, it seems likely that the federal government intends AIDA to govern substantially all development and use of AI in Canada.

With respect to extraterritorial effect, since the scope includes international trade, foreign organizations that do business in Canada or provide services to Canadians that include AI systems as defined by AIDA should consider themselves on notice as to obligations to comply with the Act.

The definition of "regulated activity" is broad, and seems intended to capture most if not all aspects of AI development and use: all "processing or making available for use any data relating to human activities for the purpose of designing, developing or using an artificial intelligence system," and all "designing, developing or making available for use an artificial intelligence system or managing its operations" falls within the definition of regulated activity (AIDA s. 5(1)).

Finally, AIDA provides that a person is responsible for an AI system if in the course of international or interprovincial trade and commerce, they design, develop or make it available for use or manage its operation (AIDA s. 5(2)). Importantly, **this means that both the designers and providers of AI systems will be subject to AIDA 's rules**, which include a variety of administrative and operational requirements.

High-impact systems, harm, and biased output

AIDA leaves the details of defining a "high-impact system" to criteria that will be established in regulations (AIDA s. 5(1)). While this strategy leaves a great deal of flexibility to respond to new uses of AI technologies as they develop, it is likely that the criteria articulated in these regulations will include or invoke the potential for harm or biased output, each of which are defined terms under AIDA.

AIDA defines harm as "(a) physical or psychological harm to an individual; (b) damage to an individual's property; or (c) economic loss to an individual" (AIDA s. 5(1)).

AIDA defines biased output as "content that is generated, or a decision, recommendation or prediction that is made, by an artificial intelligence system and that adversely differentiates, directly or indirectly and without justification, in relation to an individual on one or more of the prohibited grounds of discrimination set out in section 3 of the *Canadian Human Rights Act*, or on a combination of such prohibited grounds" (AIDA s. 5(1)). It excludes content, decisions and recommendations that have the purpose and effect of preventing, reducing or eliminating disadvantages based on or related to the prohibited grounds, that are suffered by or likely to be suffered by any group of individuals.

The first generation of these regulations might also incorporate, in some form, some or all of the impact criteria used in the federal Directive that applies to public sector entities: the rights of individuals or communities, the health or well-being of individuals or communities, the economic interests of individuals, entities, or communities, and the ongoing sustainability of an ecosystem.

Assessments and compliance monitoring

AIDA provides that a person responsible for an AI system must assess whether that system qualifies as a high-impact system under the regulations (AIDA s. 7) and maintains records of the reasons supporting their assessment (AIDA s. 10(1)). If it is a high-impact system, the person responsible must establish measures to identify, assess and mitigate the risks of harm or biased output that could result from the use of the system (AIDA s. 8), and establish measures to monitor compliance with those mitigation measures and their effectiveness (AIDA s. 9). The person responsible must maintain records of those measures as well (AIDA s. 10(1)). The content of the assessment, the mitigation measures and the compliance measures may all be set by regulation (AIDA s. 36). Clear guidance in the regulations will be of great importance here, particularly as the nature of the assessments and the mitigations to be undertaken by designers and developers may be quite different from the assessments of those making the AI systems available and/or managing their operation.

By way of preliminary guidance on what these assessments and mitigation measures might look like, organizations could cautiously consider the requirements of the federal Directive. The Directive provides for "algorithmic impact assessments" and includes mitigation measures such as human intervention in decision-making processes, third party review of the system, publishing of reviews or audits, and descriptions of training data.

Given the broad definition of "person responsible", this framework is likely intended to require the ongoing involvement of AI designers and developers in high-impact systems they create and license for use by others, in the sense that system designers may be expected to monitor or conduct audits of their customers' deployment and use of such systems. By the same token, those who make available for use or manage the operations of such systems (*e.g.*, the licensee customers of the AI system developers) must also conduct their own assessments and implement their own measures, which may simplify the auditing process for high-impact system designers.

It remains to be seen how these obligations to assess, mitigate, and monitor compliance will affect open source developers of AI (*i.e.*, those who wish to make algorithms or models available at no charge). Typically, open source developers will simply create and make their software available, take no responsibility for the use of such software by others. The wording of the criteria for determining whether a system is high-impact will therefore be of great importance for this community of developers.

Transparency

AIDA creates a nuanced transparency regime for high-impact systems that provides both for **intended use** and **actual use**.

A person who makes a system available for use must 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 mitigation measures established in respect of it; and any other information prescribed by regulation (AIDA s. 11(1)). In the absence of guidance on how the phrase "make available for use" is to be interpreted, it would be prudent for open source developers of AI who make algorithms and models for high-impact systems available for

download to the general public to consider themselves obliged to publish such information as well.

A person who manages the operation of a high-impact system must publish on a publicly-available website a plain-language description of the system that includes an explanation of (a) how the system is used; (b) the types of content that it generates and the decisions, recommendations or predictions that it makes; (c) the mitigation measures established under section 8 in respect of it; and (d) any other information prescribed by regulation (AIDA s. 11(2)).

It will be interesting to see how this transparency framework is put into practice. Making high-impact systems available for use, whether for download or on a software-as-a-service model, would trigger the obligation to publish explanations relative to *intended* uses and outputs. An organization that then makes use of that system for its own purposes and therefore "manages the operation" of such a system would also need to publish explanations, relative to *actual* uses and outputs. Such a regime could discourage mischief on the part of organizations that make use of high-impact AI systems under license, as any differences between intended use/output and actual use/output will be available for general scrutiny.

Using or making available for use anonymized information

AIDA provides that a person carrying out a regulated activity and either (i) processes or (ii) makes available for use anonymized data in the course of that activity must establish measures with respect to (a) the manner in which the data is anonymized and (b) the use or management of anonymized data (AIDA s. 6). Note that these obligations are general and not limited to high-impact systems.

Because the definition of "regulated activity" includes making available for use "any data relating to human activities for the purpose of designing, developing or using an artificial intelligence system", this may have significant implications for those providing anonymized data sets for use by AI developers.

We note that AIDA contains no definition of "anonymized data". Given that AIDA has been introduced alongside the proposed CPPA, it is reasonable to infer that the federal government intends the interpretation of this phrase to align with the defined term "anonymize" under the CPPA (CPPA s. 2(1)).

To the extent this is correct, however, we note that AIDA imposes obligations around anonymized data that the CPPA does not. Under the CPPA, once personal information has been anonymized, the act no longer applies to it (CPPA s. 6(5)). Under AIDA, by contrast, persons dealing with anonymized data in the context of a regulated activity must establish measures concerning the use and management of such data.

It may well be that those drafting AIDA consider the residual risk of reidentification, despite anonymization "in accordance with generally accepted best practices", as set out in the definition in the CPPA, is too high in the context of AI systems to permit unregulated use of such data.

In at least one respect, they may be correct, as it is possible to consider AI models that have been trained on personal information as structured collections of partially or fully anonymized data. AI models that are trained on personal information are not typically considered in themselves to represent a reidentification risk, because (crudely speaking) they contain only a "statistical residue" of the training data. For this reason, the data contained in many trained models can be regarded in a fashion similar to aggregated data – that is, effectively anonymized. Despite this, some trained models, particularly those with many parameters, have been shown to be vulnerable to "model inversion attacks" and "membership inference attacks," each of which may permit recovery of personal information.

In consequence, the provisions of AIDA that set out obligations in respect of anonymized information could be interpreted as requiring measures to mitigate or prevent model inversion and membership inference attacks. To the extent that this line of reasoning is sound, note that it has the consequence that some trained models, i.e., certain AI systems, can themselves be regarded as anonymized data. It bears repeating that these obligations would be general and not limited to high-impact systems. However, it is possible that under the regulations to come, an assessment that identifies a significant risk of model inversion or membership inference attack could, on that basis alone, qualify an AI system as a high-impact system.

Reporting material harm to the Minister

A person who is responsible for a high-impact system must, in accordance with the regulations and as soon as feasible, notify the Minister if the use of the system results or is likely to result in material harm (AIDA s. 12). As mentioned above, "harm" is defined as (a) physical or psychological harm to an individual; (b) damage to an individual's property; or (c) economic loss to an individual (AIDA s. 5(1)).

While the reporting requirement would apply to those who *intend* to create and deploy harmful systems, self-reporting by such actors is rather unlikely. The principle target of the reporting requirement is likely those persons who discover that the AI system has an unintended actual or potential harmful effect.

The inclusion of such a provision may have been inspired by the reporting requirements set out in the EU Proposed AI Regulation, but those requirements extend only to "providers" of "high-risk systems" (as defined in the EU Proposed AI Regulation), and require reporting to "market surveillance authorities". In the EU context, this makes the reporting requirement essentially an extension of the product safety / product liability framework; under the EU Proposed AI Regulation, only those who place systems on the market or put systems into service in the EU are "providers". While AIDA's reporting provision may be similarly intended to extend or supplement the Canadian product liability framework, under AIDA's expansive definition of person responsible for an AI system, designers and developers would have the same responsibilities as those actually making systems available for use.

Ministerial powers

AIDA creates a range of powers for the Minister, including the power to designate a senior official of the Minister's department to be the Artificial Intelligence and Data

Commissioner (AIDA s. 33(1)), and the power to delegate any power, duty or function conferred on the Minister other than the power to make regulations (AIDA s. 33(2)).

The general powers of the Minister include the power to (a) promote public awareness of and provide education with respect to AIDA; (b) make recommendations and prepare reports on the establishment of measures to facilitate compliance with AIDA; and (c) establish guidelines with respect to compliance (AIDA s. 32).

The Minister is also empowered to require by order:

- persons responsible for high-impact systems to provide records regarding anonymization, high-impact system assessment, mitigation and compliance measures to the Minister (AIDA ss. 10(1), 13),
- persons responsible for high-impact systems to provide additional records specified by regulation if the Minister has reasonable grounds to believe that the use of a high-impact system could result in harm or biased output (AIDA ss. 10(2), 14),
- persons responsible for AI systems to undertake audits or permit third-party audits and report the results to the Minister (AIDA s. 15),
- persons audited to implement measures to address anything referred to in the audit report (AIDA s. 16) and
- persons responsible for high-impact systems to cease using or making available the system, if the Minister has reasonable grounds to believe that the use of the system gives rise to a serious risk of imminent harm (AIDA s. 17(1)).

The Minister may also order persons responsible for AI systems or high-impact systems, as applicable, to publish any information related to the obligations regarding anonymized data, assessment, measures related to risks, monitoring, recordkeeping, publication of descriptions, notification of material harm, or audits and implementation of measures arising from audit reports (AIDA s. 18 and ss. 6-12, 15-16).

Ministerial orders may be enforced as orders of the Federal Court once a certified copy of the order has been filed (AIDA s. 20).

The Minister may also publish contraventions of AIDA on a publicly available website (AIDA s. 27) and publish information, without the consent of the person to whom the information relates and without notice to that person, that relates to an AI system if the Minister has reasonable grounds to believe that the use of the system gives rise to a serious risk of imminent harm and publication is essential to prevent the harm (AIDA s. 28).

Confidential business information

AIDA is at pains to ensure that confidentiality of trade secrets is preserved despite its relatively stringent transparency requirements and the latitude afforded to the Minister to publish information about contraventions and risks of harm.

The Minister is obliged to maintain the confidentiality of business information that has actual or potential economic value to the business or its competitors because it is not publicly available and its disclosure would result in a material financial loss to the

business or a material financial gain to their competitors (AIDA ss. 5(1), 22-23), and may disclose it only in limited circumstances, such as subpoenas, or to certain persons or bodies, such as analysts used by the Minister to administer AIDA (AIDA ss. 25, 34) or certain federal commissions (AIDA s. 26(1)).

Moreover, in requiring by order that persons responsible for AI systems publish information related to their obligations under AIDA, the law expressly notes that the Minister is not permitted to require that persons disclose confidential business information (AIDA s. 18(1)).

There is little doubt that the attention paid to the preservation of confidentiality of trade secrets in AIDA arises because of the substantial risk that explanations of how AI systems work risk disclosing those trade secrets.

A corollary benefit of this confidentiality framework is that fraudsters, hackers and other threat actors will have fewer opportunities to game the AI system or otherwise exploit weaknesses.

Enforcement

AIDA sets out a multipart enforcement scheme that echoes in part the enforcement scheme proposed in the CPPA, insofar as it sets out a scheme that includes both administrative monetary penalties (AMPs) and fines for criminal offences.

AMPs will be established by regulation, including the amounts, the designation of the provisions of AIDA the violation of which will trigger an AMP, what constitutes a minor, serious or very serious violation, and how proceedings in relation to AMPs will be undertaken and compliance agreements (AIDA s. 29). Nothing in AIDA prevents the newly created Artificial Intelligence and Data Commissioner being granted the power to apply such penalties directly.

Any organization that contravenes one of sections 6-12 of AIDA, which contain all of the key obligations imposed on persons responsible with respect to regulated activities, or who obstructs or provides false or misleading information to the Minister (or anyone acting on behalf of the Minister or an independent auditor), commits an offence that carries upon conviction a maximum of up to C$10,000,000 or 3 per cent of the organization's global gross revenues, whichever is higher (AIDA s. 30). Contraventions by employees, agents or mandataries are deemed sufficient proof of offence by the organization, unless the organization can establish that the offence was committed without its knowledge or consent (AIDA s. 30(5). A due diligence defence is also provided for, if the organization establishes that it exercised due diligence to prevent the commission of the offence (AIDA s. 30(4)).

In addition, AIDA sets out two additional, separate offences relating to personal information and making AI systems available:

- Under AIDA a person commits an offence if, for the purpose of designing, developing, using or making available for use an artificial intelligence system, the person possesses – within the meaning of subsection 4(3) of the *Criminal Code* – or uses personal information, knowing or believing that the information is

obtained or derived, directly or indirectly, as a result of the commission of an offence under an Act of Parliament or a provincial legislature, or an act or omission anywhere that, if it had occurred in Canada, would have constituted such an offence (AIDA s. 38).

- Under AIDA it is also an offence if a person without lawful excuse and knowing that or being reckless as to whether the use of an artificial intelligence system is likely to cause serious physical or psychological harm to an individual or substantial damage to an individual's property, makes the artificial intelligence system available for use and the use of the system causes such harm or damage, or with intent to defraud the public and to cause substantial economic loss to an individual, makes an artificial intelligence system available for use and its use causes that loss (AIDA s. 39).

Commission of either one of the abovementioned offences carries upon conviction a maximum of up to C$25,000,000 or 5 per cent of the organization's global gross revenues, whichever is higher (AIDA s. 40).

The offence concerning illegal use of personal information may have been introduced to align with the offence provisions of the CPPA, but may also have been put into place to discourage the activities of organizations such as Clearview AI, which harvested facial images from social media for the purposes of its facial recognition service, a practice that drew a strongly negative finding from Canadian privacy regulators in 2021 (see PIPEDA Findings #2021-001).

The offence concerning recklessly making certain AI systems available for use may be, in part, a nod to the prohibited practices set out in the EU Proposed AI Regulation, which also invokes causing physical or psychological harm to individuals, and perhaps also to the notion of "serious incident" in the EU instrument, which includes damage to property.

Next steps

Representatives of Innovation, Science and Economic Development Canada indicated, during a technical briefing following the tabling of Bill C-27, that businesses should expect a significant transition period between the adoption of the bill and its coming into force. Given the novel character of AIDA, it is also likely that the government will hold consultations and hearings in order to obtain the input of stakeholders.

While there is no guarantee that Bill C-27 and AIDA will pass in its current form, Canadian businesses utilizing AI systems in their products and services need to carefully prepare for the compliance costs and potential liability to be imposed by Canadian legislators and regulators. While Bill C-27 makes its way through Parliament, it will likely be influenced by the increasing motivation towards global harmonization of rules to guide the development, implementation and use of AI systems, and watching the evolution of the EU Proposed AI Regulation will be instructive.

We noted above that AIDA's reporting requirement may be intended to extend the existing Canadian product liability framework, but it is important to note that in any case the various requirements of that existing framework will also apply. For example, the *Canada Consumer Product Safety Act* can also be a source of exposure to manufacturers of consumer products incorporating AI technologies, as it is meant to

address and prevent dangers to human health or safety that are posed by consumer products in Canada. Moreover, the provinces and federal government have jurisdiction over various areas in which AI systems are making their way to market, such as motor vehicles (including autonomous vehicles), and medical devices. With the advent of AIDA, the layering of regulatory legal obligations is thickening.

The bottom line is: watch this space. While AIDA may be modified to some extent in committee, it is wrapped up in the same bill as a major private sector privacy law reform which is widely regarded as long overdue. Moreover, there is a worldwide impetus to regulate the development and use of AI in the near term, given its rapid penetration into a variety of sectors. In consequence, the chances that AIDA becomes law are good. While a transition period may be provided for, now is the time to future-proof your operations to ensure that your business is prepared for the coming wave of AI regulation in Canada.

[1] *Proposal for a Regulation of the European Parliament and Of The Council Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts*, COM/2021/206 final, April 21, 2021.

By

Max Jarvie, George R. Wray, Simon Du Perron, Daniel-Nicolas El Khoury

Expertise

Cybersecurity, Privacy & Data Protection, Products Law, Artificial Intelligence (AI)

Montréal

1000 De La Gauchetière Street West
Suite 900
Montréal, QC, Canada
H3B 5H4

T 514.954.2555
F 514.879.9015

Toronto

Bay Adelaide Centre, East Tower
22 Adelaide Street West
Toronto, ON, Canada
M5H 4E3

T 416.367.6000
F 416.367.6749