Torkin Manes
Barristers & Solicitors

Article

Technology, Privacy & Data Management

July 2022

Canada's First AI Act Proposed

By Lisa R. Lifshitz

On June 16, 2022, Canada's Minister of Innovation, Science and Industry ("Minister") tabled the *Artificial Intelligence and Data Act* (the "AI Act"), Canada's first attempt to formally regulate certain artificial intelligence systems as part of the sweeping privacy reforms introduced by Bill C-27.[1]

The avowed purpose of the AI Act stems from a desire to regulate certain types of AI systems and ensure that developers and operators of such systems adopt measures to mitigate various risks of harm and avoid *biased output* (as such term is defined in the Act).[2] The AI Act also establishes prohibitions related to the possession or use of illegally obtained personal information for the purpose of designing, developing, using or making available for use an AI system if its use causes serious harm to individuals.

The AI Act applies to artificial intelligence data processors, designers, developers, and those who make available artificial intelligence systems that are designated by regulation (to follow) as "high-impact systems." The AI Act broadly defines an "*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.

Interestingly, the proposed AI Act does not apply to various Canadian federal government institutions or their AI systems, including products, services, or activities that are under the direction or control of certain Canadian government departments, including:

1. the Minister of National Defence;
2. the Canadian Security Intelligence Service, Canada's domestic intelligence agency;
3. the Communications Security Establishment (Canada's equivalent organization to the NSA); or
4. other federal or provincial departments or agencies as will be further defined in the regulations.

Under the AI Act, a person (which includes a trust, a joint venture, a partnership, an unincorporated association, and any other legal entity) who is responsible for an AI system must assess whether an AI system is a "*high-impact system.*" Any person who is responsible for a high-impact system then, in accordance with (future) regulations, must:

1. Establish measures to identify, assess, and mitigate risks of harm or biased output that could result from the use of the system ("Mitigation Measures");
2. Establish measures to monitor compliance with the Mitigation Measures;
3. Keep records in general terms of the Mitigation Measures (including their effectiveness in mitigating any risks of harm/biased output) and the reasons supporting whether the system is a high-impact system;
4. Publish, on a publicly available website, a plain language description of the AI system and how it is intended to be used, the types of content that it is intended to generate, and the recommendations, decisions, or predictions that it is intended to make, as well as the Mitigation Measures in place and other information prescribed in the regulations (there is a similar requirement applicable to persons managing the operation of such systems); and
5. As soon as feasible, notify the Minister if use of the system results or is likely to result in material harm.

It should be noted that "*harm*" under the AI Act means physical or psychological harm to an individual; damage to an individual's property; or economic loss to an individual.

If the Minister has reasonable grounds to believe that the use of a high-impact system by an organization or individual could result in harm or *biased output*, the Minister has a variety of remedies at their disposal, including:

1. Ordering persons responsible for AI systems (i.e. designers, developers or those who make available for use the artificial intelligence system or manage its operation) to provide records as described above;
2. Conducting an audit of the proposed contravention or engage the services of an independent auditor to conduct the audit (and the person who is audited must provide the Minister with the audit report and pay for the audit);
3. Ordering persons responsible for AI systems to implement measures to address anything referred to in the audit report; and
4. Ordering persons responsible for AI system to cease using it or making it available for use if the Minister has reasonable grounds to believe that the use of the system gives rise to a serious risk of imminent harm.

Seeking to balance the desire for increased transparency regarding artificial intelligence systems (and avoid the so-called "black box" phenomenon) against protecting/promoting business interests, the Minister can also order the publication of certain information regarding the AI system but is not allowed to publish the *confidential business information* of a person and the Minister must take measures to maintain the confidentiality of persons' business confidential information.[3]

That being said, the AI Act contains a number of exemptions that allows the Canadian Federal Government to share and disclose confidential business information regarding a particular AI system, including with specific government departments (including the federal Privacy Commissioner and the Canadian Human Rights Commission) and provincial counterparts. Additionally, the Minister may publish information related to an artificial intelligence system on a publicly available website, without the consent of the person to whom the information relates and without notifying that person, if the Minister has reasonable grounds to believe that the use of the system gives rise to a serious risk of imminent harm; and the publication of the information is essential to prevent the harm. The AI Act again provides that no confidential business information can be published through this method.

In keeping with the other reforms proposed under Bill 27, the AI Act introduces very stiff penalties for non-compliance, which are much higher than those currently available in Canada. Firstly, there will be

administrative monetary penalties ("AMPs") that will be levied for non-compliance, but the amounts for these will be determined under forthcoming regulations (the AI Act notes that the purpose of AMPs is "*to promote compliance with this Part and not to punish*").

The AI Act also imposes fines for persons who violate Sections 6-12 of the Act (which contains obligations related to assessment, monitoring mitigation activities, etc. discussed above) or who obstructs—or provides false or misleading information to—the Minister, anyone acting on behalf of the Minister, or an independent auditor in the exercise of their powers or performance of their duties or functions. If the person is an individual, the person is liable on conviction on indictment to a fine at the court's discretion, or on summary conviction to a fine of up to $50,000 CAD. If the person is not an individual, the person is liable on conviction on indictment to a fine of up to the greater of $10 million CAD or 3% of the person's gross global revenues in its financial year before the one in which the person is sentenced. On summary conviction, a person that is not an individual is liable to a fine of up to the greater of $5 million CAD or 2% of the person's gross global revenues in the person's financial year before the sentencing.

The AI Act also establishes general offences regarding AI systems for misuse of *personal information* (which is defined under Bill C-27 as "*information about an identifiable individual*").

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 or uses personal information, knowing or believing that the information is obtained or derived, directly or indirectly, as a result of the commission in Canada 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.

Moreover, it is also an offence if the 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.

Every person who commits an offence under the above provisions of the AI Act risks even more severe fines and possible jail time. If the person is an individual, the person is liable on conviction on indictment to a fine at the court's discretion or imprisonment up to five years less a day, or both. If the person is not an individual, the person is liable on conviction on indictment to a fine of up to the greater of $25 million CAD or 5% of the person's gross global revenues in the person's financial year before sentencing. If the person is an individual, the person is liable on summary conviction to a fine of up to $100,000 CAD or imprisonment up to two years less a day, or both. If the person is not an individual, the person is liable on summary conviction to a fine of up to the greater of $20 million CAD or 4% of the person's gross global revenues in the person's financial year before sentencing.

While drafted at a high level with much detail to follow in forthcoming regulations, there is no doubt that the AI Act represents an absolute sea change in the proposed regulation of certain artificial intelligence systems in Canada. Until now, there has not been any attempt to have a targeted statute focusing on the mitigation of bias in Canadian artificial intelligence systems *per se* and to date, Canadians have instead relied on a patchwork of existing privacy, human rights, and employment legislation and various ethical guidelines and model codes established by diverse institutions, such as the Montreal Declaration for a Responsible Development of Artificial Intelligence spearheaded by the Université de Montréal,[4] to protect their interests. While the AI Act is currently only in its first reading, this Act represents a significant change in how Canadian developers and operators of certain AI systems must begin to proactively address certain harms and unintended consequences that this dynamic technology may inadvertently bring or otherwise face significant consequences.

This article was originally published in *business law today.*

1. *An Act to enact the Consumer Privacy Protection Act and the Personal Information and Data Protection Tribunal Act and to make consequential and related amendments to other Acts, also known*

as the Digital Charter Implementation Act, 2022 (First Session, Forty-fourth Parliament, 70-71 Elizabeth II, 2021-2022, First Reading, June 16, 2022). Bill 27 is comprised of three parts: Part 1 will enact the *Consumer Privacy Protection Act* and is intended to repeal Part 1 of Canada's federal private sector *Personal Information Protection and Electronic Documents Act*; Part 2 will enact the Personal Information and Data Protection Tribunal Act, which establishes an administrative tribunal to hear appeals of certain decisions made by the federal Privacy Commissioner under the *Consumer Privacy Protection Act*; and Part 3 will enact the *Artificial Intelligence and Data Act*. ↑

2. The AI Act defines *"biased output"* to mean 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. It does not include content, or a decision, recommendation, or prediction, the purpose and effect of which are to prevent disadvantages that are likely to be suffered by, or to eliminate or reduce disadvantages that are suffered by, any group of individuals when those disadvantages would be based on or related to the prohibited grounds. ↑

3. "*Confidential business information*" is defined in the AI Act as business information that (a) is not publicly available; (b) in respect of which the person has taken measures that are reasonable in the circumstances to ensure that it remains not publicly available; and (c) has actual or potential economic value to the person or their competitors because it is not publicly available and its disclosure would result in a material financial loss to the person or a material financial gain to their competitors. ↑

4. For a more detailed discussion of the existing patchwork of AI laws and model codes in Canada, see, Lisa R. Lifshitz and Myron Mallia-Dare, "Artificial Intelligence in Canada," chapter 25 of The Law of Artificial Intelligence and Smart Machines, Theodore F. Claypoole, editor, American Bar Association, 2019. ↑

Author

Lisa R. Lifshitz
Partner

Tel: 416 775 8821
llifshitz@torkinmanes.com

Lisa R. Lifshitz is a partner of the firm in Torkin Manes' Business Law Group, specializing in technology and privacy law, and is the leader of the firm's Technology, Privacy and Data Management Group. She has been nationally and internationally recognized for her technology law expertise and enjoys writing and speaking on technology law issues. She is the past president of the Canadian IT Law Association.