fogler rubinoff | David Young Law
Privacy and Regulatory Law Counsel

Comparison of key provisions in
Canada's proposed *Artificial Intelligence and Data Act* (Canada's **AIDA**) to their counterparts in the EU's proposed *Artificial Intelligence Act* (EU's **AI Act**)
Last updated August 3, 2022
Prepared by Bill Hearn, Foglers and David Young, David Young Law (with help from Max Samuels a Summer Law Student at Foglers)

	Canada's AIDA (the "Act")	**EU's AI Act (the "Act" /"Regulation")**
Purpose/objective	Section 4 - Purposes The purposes of this Act are: (a) to regulate international and interprovincial trade and commerce in AI systems by establishing common requirements, applicable across Canada, for the design, development and use of those systems; and (b) to prohibit certain conduct in relation to AI systems that may result in serious harm to individuals or harm to their interests.	Article 1- Subject Matter This Act lays down: (a) harmonised rules for the placing on the market, the putting into service and the use of AI systems in the Union; (b) prohibitions of certain AI practices; (c) specific requirements for high-risk AI systems and obligations for operators of such systems; (d) harmonised transparency rules for AI systems intended to interact with natural persons, emotion recognition systems and biometric categorisation systems, and AI systems used to generate or manipulate image, audio or video content; and (e) rules on market monitoring and surveillance. 1.4. - Objectives The general objective of the Act is to ensure the proper functioning of the single market by creating the conditions for the development and use of trustworthy AI in the Union. The specific objectives of this Act are to: (a) ensure that AI systems placed and used on the Union market are safe and respect existing law on fundamental rights and Union values; (b) ensure legal certainty to facilitate investment and innovation in AI; (c) enhance governance and effective enforcement of existing law on fundamental rights and safety requirements applicable to AI systems; and (d) facilitate the development of a single market for lawful, safe and trustworthy AI applications and prevent market fragmentation.
Definition of AI system	Section 2 - Definitions ***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.	Article 3 - Definitions ***'artificial intelligence system'*** means software that is developed with one or more of the techniques and approaches listed in Annex I and can, for a given set of human-defined objectives, generate outputs such as content, predictions, recommendations, or decisions influencing the environments they interact with. Annex I - AI Techniques and Approaches

	Canada's AIDA (the "Act")	EU's AI Act (the "Act" /"Regulation")
		(a) machine learning approaches, including supervised, unsupervised and reinforcement learning, using a wide variety of methods including deep learning; (b) logic- and knowledge-based approaches, including knowledge representation, inductive (logic) programming, knowledge bases, inference and deductive engines, (symbolic) reasoning and expert systems; and (c) statistical approaches, Bayesian estimation, search and optimization methods.
Application	Section 3(1) – Non-application AIDA does not apply with respect to a government institution as defined in s.3 of the *Privacy Act*. Section 3(2) – Product, service or activity AIDA does not apply with respect to a product, service or activity that is under the direction or control of: (a) the Minister of National Defence; (b) the Director of the Canadian Security Intelligence Service; (c) the Chief of the Communications Security Establishment; or (d) any other person who is responsible for a federal or provincial department or agency and who is prescribed by regulation.	Article 2 – Scope The Act applies to: (a) providers placing on the market or putting into service AI systems in the Union, irrespective of whether those providers are established within the Union or in a third country; (b) users of AI systems located within the Union; and (c) providers and users of AI systems that are located in a third country, where the output produced by the system is used in the Union. The Act does not apply to: (a) AI systems developed or used exclusively for military purposes; or (b) public authorities in a third country or international organisations that use AI systems in the framework of international agreements for law enforcement and judicial cooperation with the Union or with one or more Member States. Chapter 3 – Obligations of Providers and Users of High-Risk AI Systems and Other Parties Places horizontal obligations on providers of high-risk AI systems, but also establishes proportionate obligations for users and other players within the AI value chain, such as importers, distributors and authorized representatives.
Risk-based approach	Section 5(1) - Definitions ***high-impact system*** means an artificial intelligence system that meets the criteria for a high-impact system that are established in regulations.	Articles 5, 6 and 7 The "**risk ladder**" is the following: (a) unacceptable-risk AI systems are expressly prohibited (Article 5); (b) high-risk AI systems are subject to mandatory requirements and an *ex-ante* conformity assessment (Articles 6 and 7); (c) limited risk AI systems are only subject to specific transparency obligations (Article 52); and (d) low/minimal risk AI systems that fall outside the scope of regulation can be freely used.
High-impact systems	Section 7 – Assessment – high-impact system A person who is responsible for an AI system must, in accordance with the regulations, assess whether it is a high-impact system.	Article 6 – Classification rules for high-risk AI systems Irrespective of whether an AI system is placed on the market or put into service independently from the products referred to in points (a) and (b), that AI system shall be considered high-risk where: (a) the AI system is intended to be used as a safety component of a product, or is itself a

	Canada's AIDA (the "Act")	EU's AI Act (the "Act" /"Regulation")
		product, covered by the Union harmonisation legislation listed in Annex II; and (b) the product whose safety component is the AI system, or the AI system itself as a product, is required to undergo a third-party conformity assessment with a view to the placing on the market or putting into service of that product pursuant to Union harmonisation legislation. In addition to the high-risk AI systems referred to above, AI systems referred to in Annex III shall also be considered high-risk. Annex III – High-Risk AI Systems Referred to in Article 6(2) Specific types of AI systems are listed under the following categories and pre-emptively considered high risk: 1) Biometric identification and categorisation of natural persons; 2) Management and operation of critical infrastructure; 3) Education and vocational training; 4) Employment, workers management and access to self-employment; 5) Access to and enjoyment of essential private services and public services and benefits; 6) Law enforcement; 7) Migration, asylum and border control management; and 8) Administration of justice and democratic processes.
Requirements for high-impact systems	Section 6 - Anonymized data (a) A person who carries out any regulated activity and who processes or makes available for use anonymized data in the course of that activity must, in accordance with the regulations, establish measures with respect to (i) the manner in which data is anonymized; and (ii) the use or management of anonymized data. Section 7 - Assessment - high-impact system (a) A person who is responsible for an AI system must, in accordance with the regulations, assess whether it is a high-impact system. Section 8 - Measures related to risks (a) A person who is responsible for a high-impact system must, in accordance with the regulations, establish measures to identify, assess and mitigate the risks of harm or biased output that could result from the use of the system.	Chapter 2 – Requirements for High-Risk Systems High-risk AI systems must comply with the following summarized requirements: (a) Risk-management system (i) a risk management system shall be established, implemented, documented and maintained in relation to high-risk AI systems. (ii) the risk management system shall consist of a continuous process run throughout the entire lifecycle of a high-risk AI system, requiring regular systematic updating. It shall comprise the following steps: (a) identification and analysis of the known and foreseeable risks associated with each high-risk AI system; (b) estimation and evaluation of the risks that may emerge when the high-risk AI system is used in accordance with its intended purpose and under conditions of reasonably foreseeable misuse; (c) evaluation of other possibly arising risks based on the analysis of data gathered from the post-market monitoring system referred to in Article 61; (d) adoption of suitable risk management measures in accordance with the provisions of paragraphs 3 to 9 of Article 9.

	Canada's AIDA (the "Act")	EU's AI Act (the "Act" /"Regulation")
	Section 9 - Monitoring of mitigation measures (a) A person who is responsible for a high-impact system must, in accordance with the regulations, establish measures to monitor compliance with the mitigation measures they are required to establish under section 8 and the effectiveness of those mitigation measures. Section 10 - Record-Keeping (a) A person who carries out any regulated activity must, in accordance with the regulations, keep records describing in general terms, as the case may be, (i) the measures they establish under sections 6, 8 and 9; and (ii) the reasons supporting their assessment under section 7. Section 11 - Publication of description - making system available for use (a) A person who makes available for use a high-impact system must, in the time and manner that may be prescribed by regulation, publish on a publicly available website a plain-language description of the system that includes an explanation of (i) how the system is intended to be used; (ii) the types of content that it is intended to generate and the decisions, recommendations or predictions that it is intended to make; (iii) the mitigation measures established under section 8 in respect of it; and (iv) any other information that may be prescribed by regulation. Section 12 - Notification of material harm (a) 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.	(b) Data and data governance (i) training, validation and testing data sets shall be subject to appropriate data governance and management practices. Those practices shall concern in particular: (a) the relevant design choices; (b) data collection; (c) relevant data preparation processing operations, such as annotation, labelling, cleaning, enrichment and aggregation; (d) the formulation of relevant assumptions, notably with respect to the information that the data are supposed to measure and represent; (e) a prior assessment of the availability, quantity and suitability of the data sets that are needed; (f) examination in view of possible biases; (g) the identification of any possible data gaps or shortcomings, and how those gaps and shortcomings can be addressed. (c) Technical documentation (i) the technical documentation of a high-risk AI system shall be drawn up before that system is placed on the market or put into service and shall be kept up-to-date. (ii) the technical documentation shall be drawn up in such a way to demonstrate that the high-risk AI system complies with the requirements set out in this Chapter and provide national competent authorities and notified bodies with all the necessary information to assess the compliance of the AI system with those requirements. It shall contain, at a minimum, the elements set out in Annex IV. (d) Record-keeping (i) high-risk AI systems shall be designed and developed with capabilities enabling the automatic recording of events ('logs') while the high-risk AI systems are operating. Those logging capabilities shall conform to recognised standards or common specifications. (ii) for high-risk AI systems performing biometric identification and categorisation of natural person), the logging capabilities shall provide, at a minimum: (a) recording of the period of each use of the system (start date and time and end date and time of each use); (b) the reference database against which input data has been checked by the system; (c) the input data for which the search has led to a match; and (d) the identification of the natural persons involved in the verification of the results, as referred to in Article 14 (5). (e) Transparency and provision of information to users (i) high-risk AI systems shall be designed and developed in such a way to ensure that their operation is sufficiently transparent to enable users to interpret the system's output and use it appropriately. An appropriate type and degree of transparency

	Canada's AIDA (the "Act")	EU's AI Act (the "Act" /"Regulation")
		shall be ensured, with a view to achieving compliance with the relevant obligations of the user and of the provider under the Regulation. (f) Human oversight (i) high-risk AI systems shall be designed and developed in such a way, including with appropriate human-machine interface tools, that they can be effectively overseen by natural persons during the period in which the AI system is in use. (ii) human oversight shall aim at preventing or minimising the risks to health, safety or fundamental rights that may emerge when a high-risk AI system is used in accordance with its intended purpose or under conditions of reasonably foreseeable misuse. (g) Accuracy, robustness and cybersecurity (i) high-risk AI systems shall be designed and developed in such a way that they achieve, in the light of their intended purpose, an appropriate level of accuracy, robustness and cybersecurity, and perform consistently in those respects throughout their lifecycle. (ii) high-risk AI systems shall be resilient as regards errors, faults or inconsistencies that may occur within the system or the environment in which the system operates, in particular due to their interaction with natural persons or other systems.
Prohibited AI systems	AIDA does not include an outright ban of AI systems carrying on unacceptable risk.	Article 5 – Prohibited AI Practices The following AI practices shall be prohibited: (a) the placing on the market, putting into service or use of an AI system that deploys subliminal techniques beyond a person's consciousness in order to materially distort a person's behaviour in a manner that causes or is likely to cause that person or another person physical or psychological harm; (b) the placing on the market, putting into service or use of an AI system that exploits any of the vulnerabilities of a specific group of persons due to their age, physical or mental disability, in order to materially distort the behaviour of a person pertaining to that group in a manner that causes or is likely to cause that person or another person physical or psychological harm; (c) the placing on the market, putting into service or use of AI systems by public authorities or on their behalf for the evaluation or classification of the trustworthiness of natural persons over a certain period of time based on their social behaviour or known or predicted personal or personality characteristics, with the social score leading to either or both of the following: (i) detrimental or unfavourable treatment of certain natural persons or whole groups in social contexts which are unrelated to the contexts in which the data was originally generated or collected; (ii) detrimental or unfavourable treatment of certain natural persons or whole groups that is unjustified or disproportionate to their social behaviour or its gravity; (d) the use of 'real-time' remote biometric identification systems in publicly accessible spaces for the purpose of law enforcement, unless and only as much as such use is strictly necessary for one of the following objectives:

	Canada's AIDA (the "Act")	EU's AI Act (the "Act" /"Regulation")
		(i) the targeted search for specific potential victims of crime, including missing children; (ii) the prevention of a specific, substantial and imminent threat to the life or physical safety of natural persons or of a terrorist attack; (iii) the detection, localisation, identification or prosecution of a perpetrator or suspect of a criminal offence referred to in Article 2(2) of Council Framework Decision 2002/584/JHA and punishable in the Member State concerned by a custodial sentence or a detention order for a maximum period of at least three years, as determined by the law of that Member State.
Transparency	Section 11 – Publication of description – making system available for use A person who makes available for use a high-impact system must, in the time and manner that may be prescribed by regulation, 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 under section 8 in respect of it; and (d) any other information that may be prescribed by regulation.	Article 52 – Transparency obligations for certain AI systems Providers shall ensure that AI systems intended to interact with natural persons are designed and developed in such a way that natural persons are informed that they are interacting with an AI system, unless this is obvious from the circumstances and the context of use. Users of an emotion recognition system or a biometric categorisation system shall inform the natural persons exposed to it of the operation of the system. Users of an AI system that generates or manipulates image, audio or video content that appreciably resembles existing persons, objects, places or other entities or events and would falsely appear to a person to be authentic or truthful (e.g., 'deep fake'), shall disclose that the content has been artificially generated or manipulated. See also: item (e) above under Chapter II – Requirements for High-Risk Systems – Transparency and provision of information to users.
Confidentiality	Section 5 - Definitions ***confidential business information***, in respect of a person to whose business or affairs the information relates, means business information: (a) that 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) that 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. Section 24 – Disclosure of confidential business information The Minister may disclose confidential business information for the purpose of complying with a subpoena or warrant issued or order made by a court, person or body with jurisdiction to compel the production of information or for the purpose of complying with rules of court relating to the production of information.	Article 70 – Confidentiality National competent authorities and notified bodies involved in the application of this Act shall respect the confidentiality of information and data obtained in carrying out their tasks and activities in such a manner as to protect, in particular: (a) intellectual property rights, and confidential business information or trade secrets of a natural or legal person, including source code, except the cases referred to in Article 5 of Directive 2016/943 on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure apply; (b) the effective implementation of this Regulation, in particular for the purpose of inspections, investigations or audits; (c) public and national security interests; and (d) the integrity of criminal or administrative proceedings. *[See official text of draft Regulation for corrected typo in this table.]* Without prejudice to the above, information exchanged on a confidential basis between the national competent authorities and between national competent authorities and the Commission shall not be disclosed without the prior consultation of the originating national competent authority and the user when high-risk AI systems referred to in points 1 (biometric identification and categorisation of

	Canada's AIDA (the "Act")	EU's AI Act (the "Act" /"Regulation")
	Section 26 – Disclosure of information The Minister may disclose personal information or confidential business information to relevant Commissioners only if: (a) the Minister has reasonable grounds to believe that a person who carries out any regulated activity has contravened, or is likely to contravene, another Act of Parliament or a provincial legislature that is administered or enforced by the intended recipient of the information and if the information is relevant to the intended recipient's powers, duties or functions under that Act; (b) the Minister is satisfied that the disclosure is necessary for the purposes of enabling the recipient to administer or enforce the Act in question; and (c) the recipient agrees in writing to maintain the confidentiality of the information except as necessary for any of those purposes.	natural persons), 6 (law enforcement) and 7 (migration, asylum and border control management) of Annex III are used by law enforcement, immigration or asylum authorities, when such disclosure would jeopardize public and national security interests. The Commission and Member States may exchange, where necessary, confidential information with regulatory authorities of third countries with which they have concluded bilateral or multilateral confidentiality arrangements guaranteeing an adequate level of confidentiality.
Risk management	Section 8 – Measures related to risks A person who is responsible for a high-impact system must, in accordance with the regulations, establish measures to identify, assess and mitigate the risks of harm or biased output that could result from the use of the system.	Article 9 – Risk management system Regulates the establishment, implementation and documentation of a risk management system, which must be properly managed throughout the entire life cycle of high-risk AI systems. This mechanism is described as a continuous process aimed at identifying the foreseeable risks of high-risk AI systems—as well as other possible threats arising from post-market monitoring data—and suitable measures to manage all these risks.
Oversight	Section 31 - Designation The Governor in Council (Cabinet) may designate any member of the Queen's Privy Council for Canada to be the Minister for the purposes of this Part. Section 32 – General powers of Minister The general powers of Minister are to: (a) promote public awareness of this Act and provide education with respect to it; (b) make recommendations and cause to be prepared reports on the establishment of measures to facilitate compliance with this Part; and (c) establish guidelines with respect to compliance with this Part. Section 33 – Artificial Intelligence and Data Commissioner The Minister may designate a senior official of the department over which the Minister presides to be the Artificial Intelligence and Data Commissioner, whose role is to assist the Minister in the administration and enforcement of this Part.	Articles 56, 57 and 59 Articles 56 and 57 lay the foundations for the European Artificial Intelligence Board ("**EAIB**") , a new body that comprises representatives from the Member States and the European Data Protection Supervisor. The European Commission chairs the EAIB, convenes the meetings and prepares the agenda. Article 59 requires each Member State to establish or designate national competent authorities for the purpose of ensuring proper application of the Act. Such authorities are subject to strict requirements of independence, objectivity and impartiality, and each Member State must provide their authorities with adequate financial, technical and human resources to fulfil their tasks.

	Canada's AIDA (the "Act")	EU's AI Act (the "Act" /"Regulation")
	The Minister may delegate to the Commissioner any power, duty or function conferred on the Minister under this Part, except the power to make regulations under section 37.	
Notification of material harm vs serious incident	Section 5(1) – Definitions ***harm*** means: (a) physical or psychological harm to an individual; (b) damage to an individual's property; or (c) economic loss to an individual. Section 12 – Notification of material harm 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.	Article 3 – Definitions ***'serious incident'*** means any incident that directly or indirectly leads, might have led or might lead to any of the following: (a) the death of a person or serious damage to a person's health, to property or the environment; or (b) a serious and irreversible disruption of the management and operation of critical infrastructure. Article 62 – Reporting of serious incidents and of malfunctioning Providers of high-risk AI systems placed on the Union market shall report any serious incident or any malfunctioning of those systems which constitutes a breach of obligations under Union law intended to protect fundamental rights to the market surveillance authorities of the Member States where that incident or breach occurred.
Penalties	Section 29 – Administrative monetary penalties (a) A person who is found under the regulations to have committed a violation is liable to the administrative monetary penalty established by the regulations. (b) The purpose of an administrative monetary penalty is to promote compliance with this Part and not to punish. (c) If an act or omission may be proceeded with as a violation or as an offence, proceeding with it in one manner precludes proceeding with it in the other. (d) The Governor in Council may make regulations respecting an administrative monetary penalties scheme.	5.2.2 and Title II The list of prohibited practices in Title II comprises AI systems whose use is considered unacceptable as contravening Union values, for instance by violating fundamental rights or posing a high-risk of harm to the health and safety of persons. The prohibitions cover practices that have a significant potential to manipulate persons through subliminal techniques beyond their consciousness or exploit vulnerabilities of specific vulnerable groups such as children or persons with disabilities in order to materially distort their behaviour in a manner that is likely to cause them or another person psychological or physical harm. Other manipulative or exploitative practices affecting adults that might be facilitated by AI systems could be covered by the existing data protection, consumer protection and digital service legislation that guarantee that natural persons are properly informed and have free choice not to be subject to profiling or other practices that might affect their behaviour. The proposal also prohibits AI-based social scoring for general purposes done by public authorities. Finally, the use of 'real time' remote biometric identification systems in publicly accessible spaces for the purpose of law enforcement is also prohibited unless certain limited exceptions apply. Article 71 – Penalties The following infringements shall be subject to administrative fines of up to €30 million or, if the offender is company, up to 6% of its total worldwide annual turnover for the preceding financial year, whichever is higher: (a) non-compliance with the prohibition of the AI practices referred to in Article 5; or (b) non-compliance of the AI system with the requirements laid down in Article 10. The non-compliance of the AI system with any requirements or obligations under this Regulation,

	Canada's AIDA (the "Act")	EU's AI Act (the "Act" /"Regulation")
		other than those laid down in Articles 5 and 10, shall be subject to administrative fines of up to €20 million or, if the offender is a company, up to 4% of its total worldwide annual turnover for the preceding financial year, whichever is higher. The supply of incorrect, incomplete or misleading information to notified bodies and national competent authorities in reply to a request shall be subject to administrative fines of up to €10 million or, if the offender is a company, up to 2% of its total worldwide annual turnover for the preceding financial year, whichever is higher.
Offences	Section 30 – Contravention – sections 6-12 A person who commits an offence by contravening any of the requirements in sections 6 to 12 (i.e., for anonymized data; assessing high-impact systems; establishing measures related to risks; monitoring mitigation measures; keeping records; publishing descriptions for making available for use, or managing operation of, a system; notifying where a system results, or is likely to result, in material harm) or by obstructing or providing false or misleading information to the Minister: (a) is liable, on conviction on indictment, (i) to a fine of not more than the greater of $10 million and 3% of the person's gross global revenues in its financial year before the one in which the person is sentenced, in the case of a person who is not an individual, and (ii) to a fine at the discretion of the court, in the case of an individual; or (b) is liable, on summary conviction, (i) to a fine of not more than the greater of $5 million and 2% of the person's gross global revenues in its financial year before the one in which the person is sentenced, in the case of a person who is not an individual, and (ii) to a fine of not more than $50,000, in the case of an individual. Section 38 – Possession or use of personal information Every person commits an offence if, for the purpose of designing, developing, using or making available for use an AI 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: (a) the commission in Canada of an offence under an Act of Parliament or a provincial legislature; or	Provides for administrative monetary penalties for non-compliance (see above under Article 71 – Penalties)

	Canada's AIDA (the "Act")	EU's AI Act (the "Act" /"Regulation")
	(b) an act or omission anywhere that, if it had occurred in Canada, would have constituted such an offence. Section 39 – Making system available for use Every person commits an offence if the person: (a) without lawful excuse and knowing that or being reckless as to whether the use of an AI system is likely to cause serious physical or psychological harm to an individual or substantial damage to an individual's property, makes the AI system available for use and the use of the system causes such harm or damage; or (b) with intent to defraud the public and to cause substantial economic loss to an individual, makes an AI system available for use and its use causes that loss. Section 40 - Punishment (sections 38 and 39) Every person who commits an offence under section 38 or 39 (misuse of personal information; committing harm) (a) is liable, on conviction on indictment, (i) to a fine of not more than the greater of $25 million and 5% of the person's gross global revenues in its financial year before the one in which the person is sentenced, in the case of a person who is not an individual, and (ii) to a fine in the discretion of the court or to a term of imprisonment of up to five years less a day, or to both, in the case of an individual; or (b) is liable, on summary conviction, (i) to a fine of not more than the greater of $20 million and 4% of the person's gross global revenues in its financial year before the one in which the person is sentenced, in the case of a person who is not an individual, and (ii) to a fine of not more than $100,000 or to a term of imprisonment of up to two years less a day, or to both, in the case of an individual.	