

Contracting for tech under the AI provisions of CPPA, AIDA and Law 25

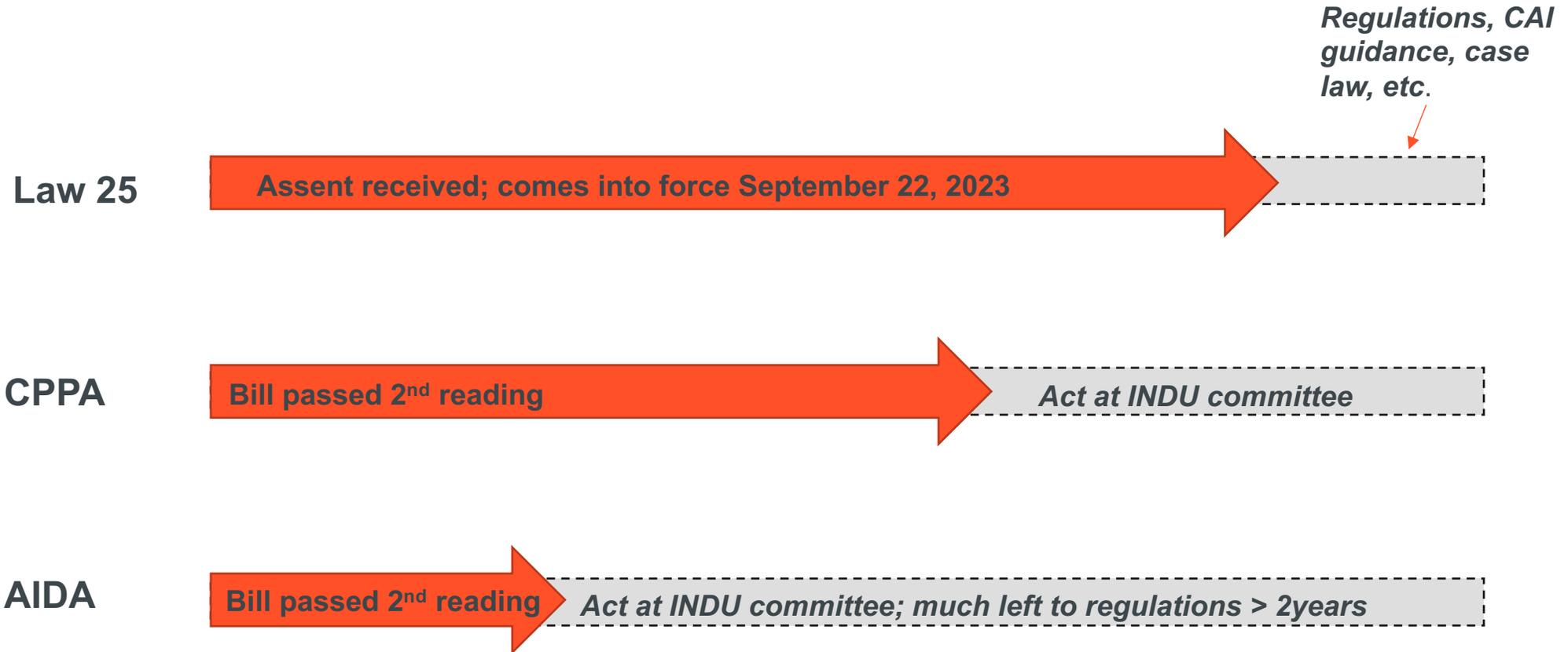
Barry Sookman & Mike Scherman

What does the dawn AI regulation look like?

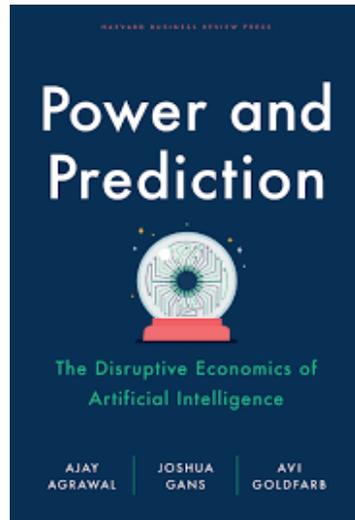


MVP1 Q. Is AI regulation at an early, nascent or late stage? A. *"AI regulation is at an early stage. Many countries are beginning to recognize the need for regulation of AI, but few have implemented any laws or policies around the technology. However, as AI becomes increasingly pervasive, governments and policymakers around the world are beginning to consider the implications of the technology and the need for legal and regulatory frameworks to ensure its safe and ethical use."* Open AI

MVP1 (Canada): AIDA, CPPA and Law 25



Contracting for uncertainty



- AI regulation will start with point solutions e.g. those that address privacy, safety and discrimination and other responsible AI principles.
- AI regulation will shift to systemic legal framework changes.
- AI regulation will trail 4th Industrial Revolution challenges.
- Future of AI regulation is unknown but will be dynamic affecting all sectors.
- Agreements need mechanisms to address evolving regulation for all markets in which business is conducted or where foreign law could apply.

Transparency and Explainability

Managing Overlapping known requirements

	Transparency at Outset	Explainability on Request
Law 25	If making a decision based <u>exclusively</u> on an automated processing of PI, but “ <u>inform the person concerned accordingly</u> ” (12.1)	If making a decision based <u>exclusively</u> on automated processing of PI, on request, must inform of <u>PI used</u> , reasons and <u>principal factors and paramaters</u> that led to decision, and <u>rights of correction</u> (12.1)
CPPA	“ <u>a general account of the organization’s use of any automated decision system to make predictions, recommendations or decisions about individuals that could have a significant impact on them</u> ” (62(2)(c))	If any automated decision system has a “ <u>significant impact</u> ” on the individual, on request must provide “ <u>an explanation of the prediction, recommendation or decision, the source of the information and the reasons or principal factors that lled to the prediction, recommendation, or decision</u> ” (62(2)(c))
AIDA	Person who manages a <u>high impact system</u> , must, in time and manner prescribe by regulation, publish a <u>description of system</u> with explanation of <u>how system is used</u> , <u>types of content generated and decisions, recommendations and predictions</u> , <u>harm mitigation measures</u> , and other information required by regs. (11(2))	None

Transparency and Explainability

	Transparency at Outset	Explainability on Request
Law 25	If making a decision based <u>exclusively</u> on an automated processing of PI, but “ <u>inform the person concerned accordingly</u> ” (12.1)	If making a decision based <u>exclusively</u> on automated processing of PI, on request, must inform of <u>PI used</u> , reasons and <u>principal factors and paramaters</u> that led to decision, and <u>rights of correction</u> (12.1)
CPPA	“ <u>a general account of the organization’s use of any automated decision system to make predictions, recommendations or decisions about individuals that could have a significant impact on them</u> ” (62(2)(c))	If any automated decision system has a “ <u>significant impact</u> ” on the individual, on request must provide “ <u>an explanation of the prediction, recommendation or decision, the source of the information and the reasons or principal factors that lled to the prediction, recommendation, or decision</u> ” (62(2)(c)) *Compare GDPR: Note applies to right of “explanation” and not right of “information”; all significant decisions, and partially automated decisions
AIDA	Person who manages a <u>high impact system</u> , must, in time and manner prescribe by regulation, publish a <u>description of system with explanation of how system is used</u> , types of content generated and	None



1. Disclosures from all vendors/providers
2. Cooperation on responding to requests
3. Covenant for best practices/standards
4. Advance notice of changes (with consent/consultation right)
5. Employee training
6. Interoperable issues

Data Anonymization

Law 25

- reasonably foreseeable in the circumstances that it irreversibly no longer allows the person to be identified directly or indirectly
- must be anonymized according to generally accepted best practices and according to the criteria and terms determined by regulation

CPPA

“irreversibly and permanently modify personal information, in accordance with generally accepted best practices, to ensure that no individual can be identified from the information, whether directly or indirectly, by any means”

AIDA

“anonymized data” A person who carries out any regulated activity and who in the course of that activity must, in accordance with the regulations, establish measures with respect to: (a) the manner in which data is anonymized; and (b) the use or management anonymized data (s.6)

Data Anonymization

Law 25

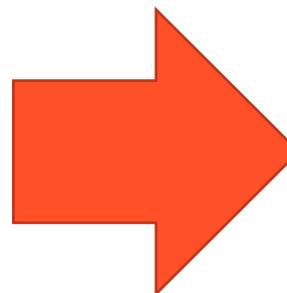
- reasonably foreseeable in the circumstances that it irreversibly no longer allows the person to be identified directly or indirectly
- must be anonymized according to generally accepted best practices and according to the criteria and terms determined by regulation

CPPA

“irreversibly and permanently modify personal information, in accordance with generally accepted best practices, to ensure that no individual can be identified from the information, whether directly or indirectly, by any means”

AIDA

“anonymized data” A person who carries out any regulated activity and who in the course of that activity must, in accordance with the regulations, establish measures with respect to: (a) the manner in which data is anonymized; and (b) the use or management anonymized data (s.6)



- Law 25 and CPPA go beyond the PIPEDA “reasonable expectations” or “reasonable foreseeable” tests under PIPEDA (and other provincial privacy laws) and beyond the GDPR “reasonably likely test”.
- AIDA has a potentially incompatible test
- AIDA’s broad definition of AI system will make many uses subject to both AIDA and CPPA.
- Contract considerations:
 - Counter-party requirement to comply with all applicable laws re anonymization including the manner in which data is anonymized, and use and management of anonymized data
 - Diligence respecting all data used for AI systems
 - Prohibition against re-identification
 - Standards for best practices for anonymization
 - Audits/inspections
 - Future proof terms
 - Handling vendor requests to use anonymized data for their own purposes
 - Indemnities, LOL

High Impact Systems (AIDA)

Assess if a “High Impact System”:

an artificial intelligence system that meets the criteria for a high-impact system that are established in regulations

Likely factors:

- Evidence of risks of harm to health and safety, or a risk of adverse impact on human rights, based on both the intended purpose and potential unintended consequences;
- The severity of potential harms;
- The scale of use;
- The nature of harms or adverse impacts that have already taken place;
- The extent to which for practical or legal reasons it is not reasonably possible to opt-out from that system;
- Imbalances of economic or social circumstances, or age of impacted persons; and
- The degree to which the risks are adequately regulated under another law.

If yes

Measures (as per regs) to identify, assess and mitigate risk of:

→ harm to individual (physical, psychological, property, economic)

→ Biased output, i.e. adversely differentiates without justification on prohibited grounds

(e.g. race, national or ethnic origin, colour, religion, age, sex, sexual orientation, gender identity or expression, marital status, family status, genetic characteristics, disability and conviction for an offence)

Maintain records of assessment and measures, as per regs

Monitor compliance with, and effectiveness of, above measures as per regs

Publish description re: high impact system as per regs

Notification of actual or likely material harm, as per regs

High Impact Systems (AIDA)

Assess if a “High Impact System”:

an artificial intelligence system that meets the criteria for a high-impact system that are established in regulations

Likely factors:

- Evidence of risks of harm to health and safety, or a risk of adverse impact on human rights, based on both the intended purpose and potential unintended consequences;
- The severity of potential harms;
- The scale of use;
- The nature of harms or adverse impacts that have already taken place;
- The extent to which for practical or legal reasons it is not reasonably possible to opt-out from that system;
- Imbalances of economic or social circumstances, or age of impacted persons; and
- The degree to which the risks are adequately regulated under another law.

If yes

Measures (as per regs) to identify, assess and mitigate risk of:

→ → harm to individual (physical, psychological, property, economic)

Biased output, i.e. adversely differentiates without justification on prohibited grounds

(e.g. race, national or ethnic origin, colour, religion, age, sex, sexual orientation, gender identity or expression, marital status, family status, genetic characteristics, disability and conviction for an offence)

Maintain records of assessment and measures, as per regs

Monitor compliance with, and effectiveness of, above measures as per regs

Publish description re: high impact system as per regs

Notification of actual or likely material harm, as per regs

What we can do:

- Set limits on use (e.g. prohibited uses)
- Cooperation within ecosystem
 - Compliance by SP
 - cooperation re: others' compliance
- Process to adapt to changes

Manage uncertainty: standards

- ISED [Companion Document](#)
 - “The risk-based approach in AIDA, including key definitions and concepts, was designed to reflect and align with evolving international norms in the AI space – including the EU AI Act, the Organization of Economic Co-operation and Development (OECD) AI Principles, and the US National Institute of Standards and Technology (NIST) Risk Management Framework (RMF) – while integrating seamlessly with existing Canadian legal frameworks. For example, the definition of artificial intelligence systems in AIDA aligns with concepts developed through the OECD that are also represented in the EU AI Act. Inter-operability with legal frameworks in other jurisdictions would also be a key consideration in the development of regulations, in order to facilitate Canadian companies' access to international markets.”
 - Evolve tech contracting practices to adopt and require counter-parties to adopt developing interoperable AI standards:
 - Governance standards (addressed to corporate leaders, admin best practices), e.g., OECD
 - Foundational standards (frameworks that can be implemented across all AI use cases e.g., ISO/IEC 22989 (AI concepts and terminology), ISO/IEC 23894 (guidance on AI risk management), OECD’s framework for AI risk classification), ISO/IEC 42001 (management system standard for artificial intelligence, considered for adoption by the EU and UK national standards bodies)
 - Technical standards e.g., U.S., NIST, U.K., Standards Hub, Japan, National Institute of Advanced Industrial Science and Technology, EU, Committee for Standardization (CEN), European Committee for Electrotechnical Standardization (CENELEC) (or CEN-CENELEC) See, [Advancing Cooperative AI Governance at the 2023 G7 Summit](#)

Extent of Liability and Remedies

Ministerial Orders	Fines/ AMPs	Criminal Offenses	Private Right of Action
Produce records (AIDA 13/14)	AMPs as established by regs (AIDA 29)	Up to \$25M/5% rev and 5 years imp. (AIDA 38 39)	Private right of action (CPPA 107)
Conduct audit (AIDA 15, CPPA 97)	Fines up to \$10M/3% rev (AIDA 30)	Up to \$25M/5% rev (CPPA 128)	Private right of action (Law 25)
Cessation of use (AIDA 17)	AMPs up to \$10M/3% rev (CPPA 95)	Up to \$25M/4% rev (Law 25 91)	
Compliance order (CPPA 93)	AMPs up to 10M/2% rev (Law 25 90)		
Orders as appropriate (Law 25 54)			

How to Manage:

- Due diligence
- Support re: audits, records, orders, etc.
- Regular monitoring/audits
- Indemnities (with procedures)

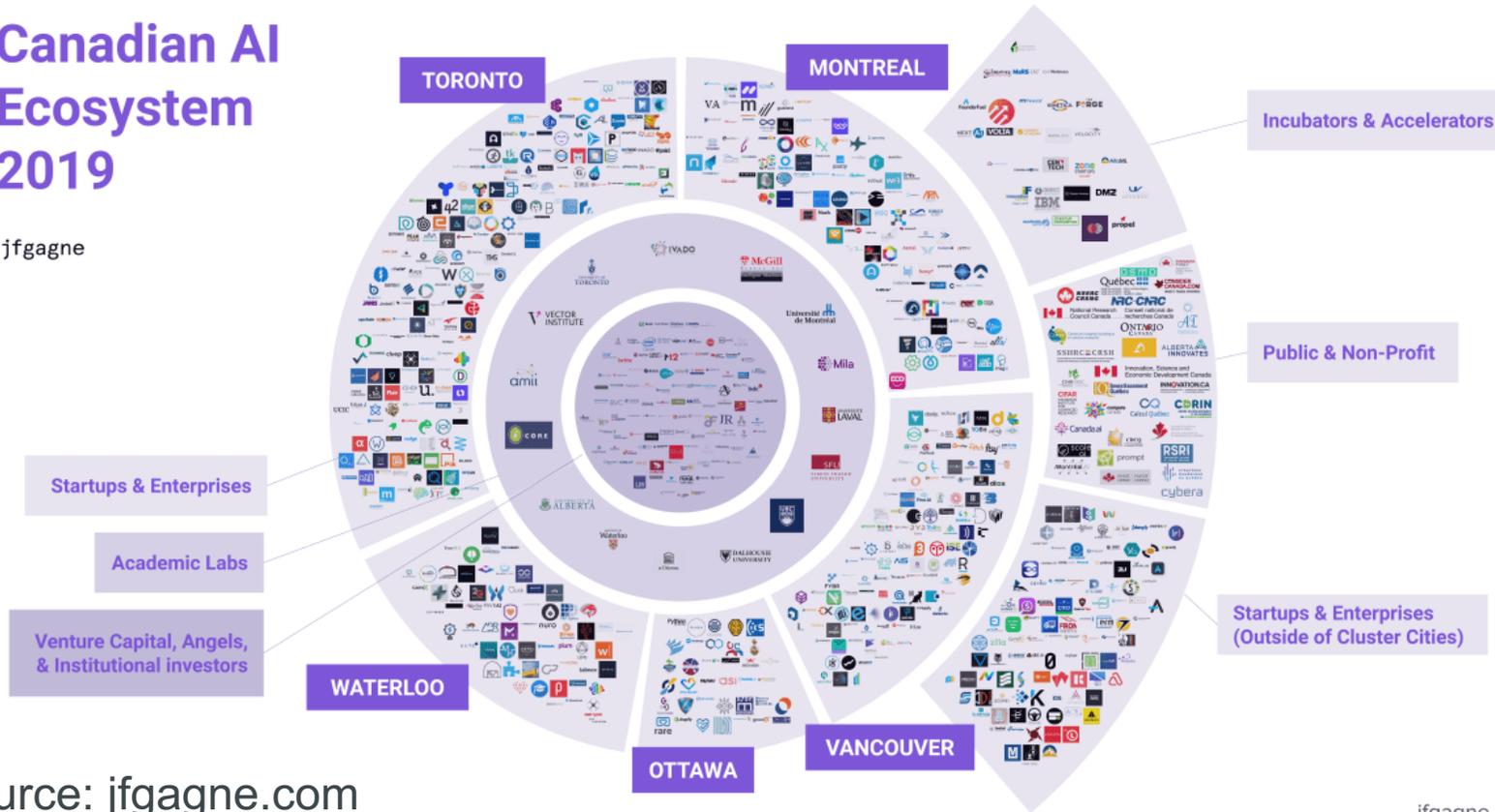
Allocating Responsibility Among AI Actors

Carries out Regulated Activity	*AIDA does not permit regs to allocate responsibilities between actors, notwithstanding Companion Document; *AIDA also applies to partly autonomous AI systems
Processes or makes available data related to human activities (applies to all AI systems)	Must in accordance with regs establish measures re manner in which data is anonymized or and use or management of anonymized data
Person Responsible – anyone who designs, develops, makes available or manages AI systems (applies to high impact systems)	Assess whether it is a high-impact system.
	Establish measures to identify, assess and mitigate the risks of harm or biased output
	Establish measures to monitor compliance with mitigation measures and the effectiveness of those mitigation measures.
	Keep records
Person who makes HIS available or who manages its operation	Must publish description of system i.e., how it is intended to be used, types of content, mitigation measures

Allocating Responsibility

Canadian AI Ecosystem 2019

jfgagne



Source: jfgagne.com

jfgagne.ai

- Must wait for AIDA amendments and regs
- Unworkable complex web of supply chain contracts to enable compliance
- Terms from downstream/upstream AI actors
- Assistance to support own compliance efforts (e.g. information, request response, etc.)
- Operational processes to coordinate overlapping areas
- Clear allocation of responsibility/liability

More from the McCarthy team....

- [Artificial intelligence \(AI\) Risks and Opportunities: AI Insights Series from McCarthy Tétrault's Cyber/Data Group](#)
- [The Dawn of AI Law: The Canadian Government Introduces Legislation to Regulate Artificial Intelligence in Canada](#)
- [AIDA's regulation of AI in Canada: questions, criticisms and recommendations](#)
- [One Step Closer to AI Regulations in Canada: The AIDA Companion Document](#)
- [AIDA Companion Document: overview and questions](#)
- [A new way to manage AI risks: The National Institute of Standards and Technology's AI Risk Management Framework](#)
- [CPPA: problems and criticisms – automated decision making](#)
- [CPPA: problems and criticisms – anonymization and pseudonymization of personal information](#)

.....and more at [McCarthy TechLex](#)