Board Ready Women: Responsible AI Governance

March 12, 2024

mccarthy tétrault

Charles Morgan

Partner

Montréal
cmorgan@mccarthy.ca
514-397-5230

Law School
McGill University

Bar Admission
Québec, 1998

Practices
Procurement
Cyber/Data
Intellectual Property

Industries
Information Technology
Fintech

Strategic Issues
Cyber/Data
Artificial Intelligence

- Charles brings deep understanding of disruptive technologies, providing practical advice to help clients fully exploit the promise of innovative solutions while managing risk.
- Charles is the national co-leader of McCarthy Tétrault's Cyber/Data Group and former leader of our Technology Law group. He is the former President of the International Technology Lawyers Association (iTechLaw).
- Charles' practice takes a 360-degree approach to data, helping clients extract the tremendous value inherent in data, while at the same time managing the associated risks. He is a recognized thought-leader on the responsible deployment of artificial intelligence.
- In addition, Charles regularly serves as "breach coach" for our clients in matters of enterprise-wide risk, including on three of the largest cyber incidents in Canadian history.

1. The Legal Landscape of AI
2. Responsible AI Governance

mccarthy tétrault

1. The Legal Landscape of AI

Automated decision-making

GDPR (European Union):

- **Article 22:** The data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her.

Bill 25 (Québec)

- **Article 12.1** Any person carrying on an enterprise who uses personal information to render a decision based exclusively on an automated processing of such information must inform the person concerned accordingly not later than at the time it informs the person of the decision.
- He must also inform the person concerned, at the latter's request,
  - (1) of the personal information used to render the decision;
  - (2) of the reasons and the principal factors and parameters that led to the decision;
  - and (3) of the right of the person concerned to have the personal information used to render the decision corrected.

Regulatory Approaches

Jurisdiction	Legislation	Key Dates	Key Approaches	Sanctions
EU	EU AI Act	**Adoption**: April 2024? **Entry into force**: Staggered approach to enforcement, becoming fully applicable by 2026 at the earliest	Risk-based: Unacceptable Risk: Prohibited High Risk: Conformity Assessment Limited Risk: Transparency + code of conduct General purpose AI models as a specific category	Up to €35 million or 7% worldwide turnover
Canada	AIDA	**Adoption**: 2024? **Entry into force**: 2025 at the earliest	Risk-based: High-Impact Systems: Governance + transparency obligations General purpose AI models as a specific category Details left to regulations (ISED)	Up to $25 million or 5% worldwide turnover + prison sentences
US	Fragmented legislative landscape: **Blueprint for an AI Bill of Rights** (Oct 2022); **Executive Orders** 13960 (Dec 2020) & 14110 (Oct 2023); **New York City's Local Law 144** re: automated employment decision tools (July 2023), etc.	Ongoing (180+ AI-related State bills since 2019)	Focus on bias mitigation and anti-discrimination Obligations for dual-use AI systems Enforcement by existing agencies (FTC, DoJ, etc.)	Varies based on regulation

High Impact Systems (ISED proposition)

(1) Employment-related determinations

(2) Decisions, recommendations, or predictions for purposes relating to access to services for individuals

(3) Biometric systems used for identification and inference about the characteristics, psychology, or behaviours of individuals.

(4) Content moderation on online platforms and content prioritization

(5) Uses in Healthcare and emergency services (Except in medical devices)

(6) Uses by a tribunal or administrative instance

(7) Uses to aid a peace officer in the exercise of their powers

High-Impact Systems

Before a high-impact system is made available the person who makes it available must ensure that (in accordance with regs)

- an assessment of the adverse impacts that could result from the intended use or from any other use of the system that is reasonably foreseeable has been carried out;
- take measures to assess and mitigate any risks of harm or biased output;
- test the effectiveness of the mitigation measures;
- permit human oversight of the AI system;
- the system is performing reliably and as intended and is robust even in adverse or unusual circumstances;
- maintain a manual on the system's operations;
- records are kept showing compliance and relating to the data and processes used in developing the high-impact system. (s10(1))

High-Impact Systems

A person who manages the operations of a high-impact system must (in accordance with regs)

- ensure that the requirements of the person who makes it available are met if there are reasonable grounds to believe that they have not been accomplished;
- establish measures to identify, assess and mitigate the risks of harm or biased output that could result from the use of the system and carry out tests of the effectiveness of the mitigation measures;
- ensure that humans are overseeing the system's operations;
- establish measures allowing users to provide feedback on the system's performance;
- if there are reasonable grounds to suspect that the use of the system has resulted, in serious harm or that the mitigation measures are not effective in mitigating risks of serious harm, assess whether the use of the system did actually result in serious harm or the measures are actually not effective in mitigating those risks and, if so, cease the system's operations until additional or modified measures are put in place that will mitigate risks of serious harm and comply with notification obligations;
- keep records demonstrating compliance. (s11(1))

General-Purpose AI Systems

— ***general-purpose system*** means an artificial intelligence system that is designed for use, or that is designed to be adapted for use, in many fields and for many purposes and activities, including fields, purposes and activities not contemplated during the system's development.

— Before a general-purpose system is made available the person who makes it available for the first time must ensure (in addition to requirements generally applicable to high-impact systems) that:

- **[Data Governance]** measures respecting the data used in developing the system have been established in accordance with regulations
- **[Transparency]** a plain-language description has been prepared of
  - the system's capabilities and limitations,
  - the risks of harm or biased output, and
  - any other information prescribed by regulation
- **[Watermarking]** if the system generates digital output consisting of text, images or audio or video content,
  - best efforts have been made so that members of the public, unaided or with the assistance of software that is publicly available and free of charge, are able to identify the output as having been generated by an artificial intelligence system, and
  - all measures prescribed by regulation have been taken so that members of the public are able to identify the output as having been generated by an artificial intelligence system;

mccarthy tétrault

Office of the Privacy Commissioner of Canada

Principles for responsible, trustworthy and privacy-protective generative AI technologies

Legal Authority and Consent - Ensure legal authority for PI collection/use. Obtain specific consent. Ensure third-party-sourced information is lawfully collected and authorized for disclosure.

Appropriate Purposes - Only collect, use, or disclose PI for appropriate purposes. Avoid creating systems leading to unfair or discriminatory treatment.

Necessity and proportionality - Establish necessity/proportionality of generative AI and PI use. Opt for anonymized, synthetic, or de-identified data when possible.

Openness - Be transparent about PI collection, use, and disclosure, and potential privacy risks.

Accountability - Ensure compliance with privacy legislation and explainable AI tools. Conduct assessments to identify/mitigate impacts on privacy and other rights.

Individual Access - Enable individuals' right to access their PI via appropriate procedures.

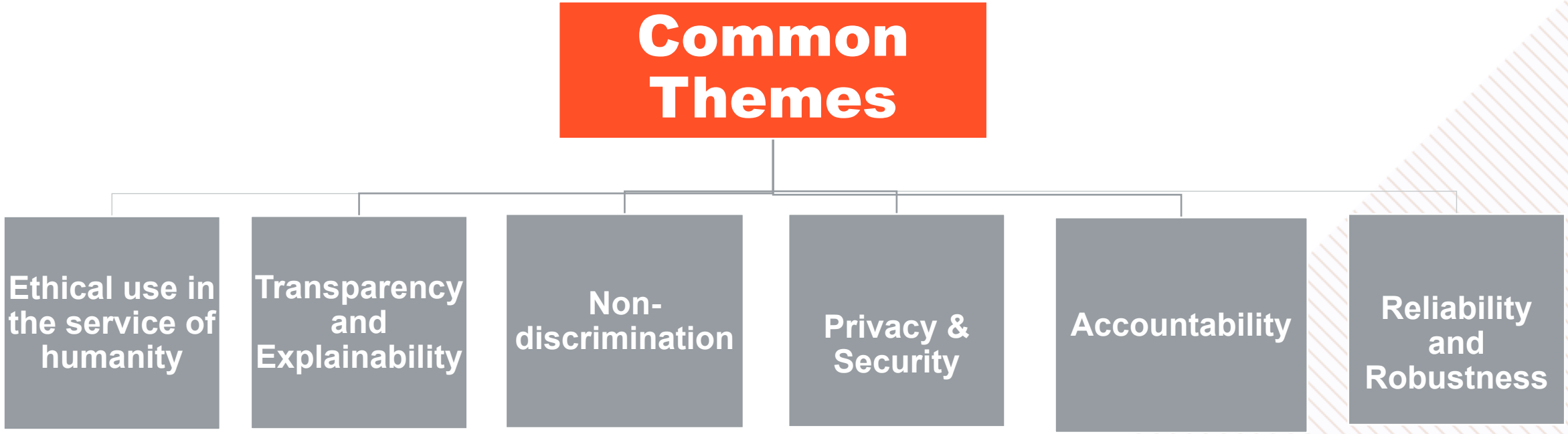
Limiting Collection, Use, and Disclosure - Limit PI collection, use, and disclosure to only what's needed for explicitly specified purposes.

Accuracy - Ensure PI is accurate, complete, and up-to-date as necessary for its intended use.

Safeguards - Establish safeguards to protect PI and mitigate privacy risks. Maintain threat awareness and design products/services to prevent inappropriate tool use.

2. Responsible AI Governance

Emerging Norms



mccarthy tetrault

Emerging International Standards

- ISO/IEC 42001 - Artificial Intelligence Management System (AIMS)
- NIST - AI Risk Management Framework
- IEEE - Recommended Practice for Organizational Governance of AI

ISO

IEEE
Advancing Technology for Humanity

NIST NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
U.S. DEPARTMENT OF COMMERCE

Responsible AI Governance

- AI Governance Committee
- AI Accountability Framework and Policies
- Responsible AI Impact Assessments
- Vendor Management
- Data Readiness and Testing
- Responsible AI by Design
- Incident Response

Accountability Frameworks (s. 12)

Accountability frameworks are meant to ensure that organizations involved in the development and deployment of both general-purpose and high-risk AI systems are accountable for their risk management practices. These frameworks must, in accordance with regulations, include:

- a description of the roles and responsibilities and reporting structure for all personnel who contribute to making the AI system available or who contribute to the management of its operations;
- policies and procedures respecting the management of risks relating to the AI system;
- policies and procedures respecting the data used by the AI system;
- a description of the training that the personnel referred to above must receive in relation to the AI system and the training materials they are to be provided with;
- if the person establishing and maintaining the framework manages the operations of the AI system, policies and procedures on how the personnel referred to above are to advise the person of any use of the AI system that results, directly or indirectly, in serious harm or of any mitigation measures that are not effective in mitigating risks of serious harm; and
- anything that is prescribed by regulation.

AI Vendor management

- Contracting in an uncertain regulatory environment requires flexibility and adaptability.
- Meeting transparency and explainability requirements will require vendor support.
  - Require applicable disclosures from all vendors/providers
  - Require cooperation on responding to requests
- Vendors will want to use client data to train models: data anonymization v. de-identification (+ different standards in different laws (e.g., AIDA and CPPA)).
  - Standards for best practices for anonymization
  - Audits/inspections
  - Future proof terms
- High impact AI systems will require specific measures for risk mitigation, record-keeping, compliance monitoring, and notification of harm.
  - Set limits on use of systems (eg. prohibited uses)
  - Implement process to adapt to changes in regulatory regime
- Liability and remedies include fines, penalties, private right of action, and compliance orders under different laws.
- Allocating responsibility among AI actors and managing supply chain implications are crucial considerations.

Questions?

THANK YOU