REGULATING AI IN CANADA: BILL C-27 AND THE AI AND DATA ACT

Dr Teresa Scassa
Canada Research Chair in Information Law and Policy
University of Ottawa

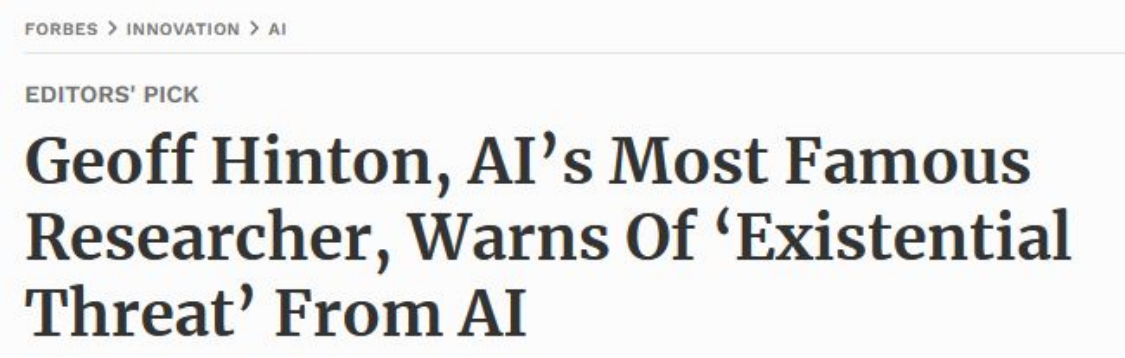
2023 CALL/ACBD Conference

May 29, 2023

Setting the AI Context

- Artificial intelligence (AI) promises to be a major driver of the global economy:
    - Prediction of global GDP increase by up to 14 % by 2030 (PwC)
    - AI could double global economic growth rates by 2035 (Accenture)
- AI is used in a very broad range of contexts and across all sectors of the economy
    - Automation of workplace, decision-making; use in policing, military; automation of vehicles; scientific research and discovery; health care; financial sector; art, journalism, film; potential uses are virtually unlimited
- Very rapid development and adoption; *fundamentally transformative in nature*
- AI technologies and systems can be opaque and may continually evolve
- All of these create substantial challenges for regulation

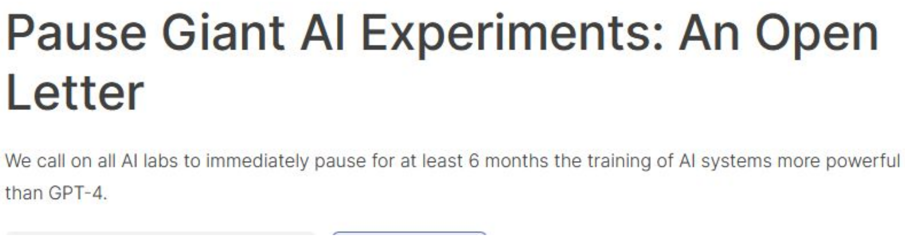
Science fiction meets reality?



FORBES > INNOVATION > AI

EDITORS' PICK

Geoff Hinton, AI's Most Famous Researcher, Warns Of 'Existential Threat' From AI



Pause Giant AI Experiments: An Open Letter

We call on all AI labs to immediately pause for at least 6 months the training of AI systems more powerful than GPT-4.

Why regulate AI?

- To reduce the risk of harm
  - Harm may take multiple forms (physical, psychological, economic, social, democratic, civil liberties, discrimination, environmental)
- To ban or prohibit certain types of tools/technologies
- To provide for transparency and accountability
- *To build trust in order to support development and use of AI*
- *To support innovation*

AI Regulation

- Principles:
  - OECD Principles and Recommendations: https://oecd.ai/en/ai-principles ; AI Policy Observatory
  - UNESCO Recommendations on the Ethics of AI: https://unesdoc.unesco.org/ark:/48223/pf0000381137
- Proposals for legislation/regulation:
  - EU AI Act
  - Canada's AI and Data Act (AIDA) in Bill C-27
  - UK's *Pro-Innovation Approach to AI Regulation*
  - China's draft regulation on AI
- Currently little international co-ordination around regulation/governance

Ex ante regulation

- *Ex ante* regulation seeks to avoid harms by setting standards for compliance prior to launch of product/service (risk regulation)
  - E.g.: some data protection obligations; medical device regulation; product safety regulation
- Tools can include
  - Regulatory frameworks
  - Directives
  - Standards
  - Codes of ethics
- Canada's *Artificial Intelligence and Data Act* (in Bill C-27) is designed as *ex ante* risk regulation
- So is Canada's *Directive on Automated Decision Making* (DADM)

Ex post regulation

- *Ex post* measures are those that apply after things go wrong
  - E.g.: tort law, privacy complaints mechanisms, human rights complaints, consumer protection recourses, competition law remedies, administrative law recourses (e.g. judicial review)
    - Can provide for redress, compensation, punishment
- An important question is the extent to which these mechanisms are adapted to the harms/challenges posed by AI
  - Common law evolves slowly
  - Complexity of AI issues will require additional resources for regulators, and likely additional powers

To legislate or not to legislate…

- The EU has proposed an AI Act, that is *detailed and prescriptive*, raising concerns that it will not be sufficiently flexible and adaptive
- Canada’s AIDA is left largely to be developed in regulations, raising concerns that Parliament will be enacting a ‘blank cheque’
- The UK is consulting on a proposal that relies heavily upon existing regulators and statutes, guided by principles, and with some room for gap filling
- The US has developed a standard – the NIST *AI Risk Management Framework* which could be adopted on a voluntary basis or adopted by legislation

Locus of regulation

- Need for international action to harmonize principles, standards and approaches
- At what level of government will regulation occur?
    - Federal states such as Canada experience particular challenges
        - Note that Quebec's innovation ministry has launched a consultation on responsible AI in Quebec through the Conseil de l'innovation du Québec
- Regulation/governance may also be by sector
    - Public vs private sector
    - By regulator (e.g., competition, privacy, human rights)
    - By industry sector (e.g., transportation, medical devices, financial sector)

Canada’s proposed Artificial Intelligence and Data Act (Bill C-27)

- Bill C-27 is currently at 2d reading in Parliament; AIDA is Part 3 of this Bill
- AIDA will apply:
  - Across the country and across sectors/industries as long as there is an element of *interprovincial or international trade and commerce*
- The AIDA does NOT apply:
  - To federal government institutions (as defined under the *Privacy Act*)
    - (Federal Directive on Automated Decision-Making will apply to the federal public sector in some circumstances)
  - To DND, CSIS, CSE or to any federal or provincial department or agency prescribed in regulations
  - To provincial public sectors (?)
- Companion document: “activities such as research or the development of methodologies are not in themselves regulated activities under AIDA”

What AIDA does not do

- Address or enhance the powers/resources of existing regulators who will be exempted from the application of AIDA
- Address the governance of AI in provincial public sectors
  - Note that Ontario has been working on a Trustworthy AI Framework
- Address *ex post facto* regimes for complaints, redress

High Risk/**High Impact** : Canada’s AIDA

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

- Key factors for determining high impact (from companion document):
  - 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.

High Risk/High Impact: EU AI Act

- EU AI Act, Art. 6 defines high risk systems, and it also refers to a list of systems in Annex III that are considered high-risk
- These include systems for:
  - Biometric identification
  - Admissions and assessment in educational institutions
  - Recruitment and/or evaluation and performance monitoring of employees
  - Allocating and overseeing public assistance benefits and services
  - Assessing creditworthiness
  - Predictive policing and profiling; assessing risk to offend or reoffend; crime analytics related to persons
  - Detecting deep fakes or assessing the reliability of evidence
  - Detecting the emotional state or truthfulness of natural persons (by government or law enforcement)
  - Use in immigration
  - Use by judges in researching and interpreting facts and the law and in applying the law to a concrete set of facts.
  - As safety components in the management and operation of road traffic and the supply of water, gas, heating and electricity
  - In dispatching emergency first response services

What are the harms to be addressed?

- Harm is defined in the AIDA to mean:
  - **(a)** physical or psychological harm to an individual;
  - **(b)** damage to an individual's property; or
  - **(c)** economic loss to an individual.
- It also addresses "biased output", which is defined in terms of discriminatory bias
- Is the concept of "harm" sufficiently broad in AIDA?
  - "Harms may be experienced by individuals independently or may be experienced broadly across groups of individuals, increasing the severity of the impact. For example, more vulnerable groups, such as children, may face greater risk of harm from a high-impact AI system and necessitate specific risk mitigation efforts." (Companion document)
- Quantifiable v. non-quantifiable harm?

Harm in the DADM

- Algorithmic Impact Assessments must take into account harm to:

  - the rights of individuals *or communities*;
  - the equality, dignity, privacy, and autonomy of individuals;
  - the health or well-being of individuals *or communities*;
  - the economic interests of individuals, *entities, or communities*;
  - the *ongoing sustainability of an ecosystem*.

High Risk/High Impact: UK approach

- UK: “Our framework is context-specific. We will not assign rules or risk levels to entire sectors or technologies. Instead, we will regulate based on the outcomes AI is likely to generate in particular applications.”

Data

- Canada (AIDA): Section 6 contains specific obligations to establish measures regarding anonymization and use/management of anonymized data in any regulated activity (These are in addition to data protection requirements in PIPEDA (or CPPA if enacted))
  - There is also a requirement to document measures established under s. 6
- There are no specific requirements in relation to *data quality*, although there are requirements to establish measures to "identify, assess and mitigate the risks of harm or biased output"

Data: EU approach

- EU *AI Act*, art. 10 contains a set of data governance requirements for high-risk AI – these are designed to address both data quality and data protection (privacy) – they are in addition to data protection requirements
- Article 10(2): 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.

Data: EU approach (cont'd)

- In addition, the EU *AI Act* requires that training, validation and testing data sets "shall be relevant, representative, free of errors and complete"
- They must also "take into account, to the extent required by the intended purpose, the characteristics or elements that are particular to the specific geographical, behavioural or functional setting within which the high-risk AI system is intended to be used"
- The use of sensitive data for the purposes of bias monitoring, detection and correction is permitted – but only with appropriate safeguards

Data: UK

- UK proposal: Reliance on existing data protection law and equality law to address data issues relating to privacy and discrimination
- Anticipates that regulators will need to:
  - "Consider the role of available technical standards, for example addressing AI safety, security, testing, data quality, and robustness (including, ISO/IEC 24029-2, ISO/IEC 5259-1, ISO/IEC 5259-3* , ISO/IEC 5259-4* , and ISO/IEC TR 5469*) to clarify regulatory guidance and support the implementation of risk treatment measures."

Transparency

- The AIDA requires those make available for use or who manage high-impact systems to publish plain language descriptions of the systems and of how they are used
  - The Minister may also require that other information be published (s. 18(1)), short of publishing any confidential commercial information
- Section 63(3) of the *Consumer Privacy Protection Act* would also require an organization that has used an automated decision system to provide a requesting individual with “an explanation of the prediction, recommendation or decision” made about them
- Under the EU *AI Act*, transparency “will be limited only to the minimum necessary information for individuals to exercise their right to an effective remedy and to the necessary transparency towards supervision and enforcement authorities, in line with their mandates”

Oversight

- EU *AI Act* requires a state to designate national competent authorities and to choose from among them a national supervisory authority
  - It also requires that the authorities are properly resourced and must be objective and impartial
- UK proposal provides for oversight by multiple existing agencies, with a role for a central authority to co-ordinate, assess, and fill gaps
- Canada's AI gives supervisory authority to the Minister of Industry
  - There is provision for an 'AI and Data Commissioner' who is a subordinate of the Minister
  - An external advisory board will advise the Minister

Enforcement - AIDA

- Under Canada’s AIDA, the Minister may order an organization to:
  - Provide it with the records kept under the AIDA
  - Conduct an audit or engage an organization to conduct an audit where there are reasonable grounds to believe there has been a contravention
  - Comply with recommendations contained in an audit report
  - Cease using a high impact system if there are reasonable grounds to believe there is a serious risk of imminent harm
  - Publish certain information
- The Minister may also impose administrative monetary penalties (AMPs)
- Breaches of the AIDA can also be treated as offences

Enforcement – EU AI Act

- Enforcement will lie with the designated national competent authorities
- AI-specific powers will include the power to investigate compliance with obligations, the ability to order corrective actions, and to order that a system be removed from the market either permanently or temporarily
- Substantial administrative monetary penalties may be imposed for non-compliance with certain EU AI Act requirements relating to prohibited systems and data governance obligations

Enforcement – UK proposal

- Enforcement will largely be via existing regulatory authorities who may receive some enhanced powers and competencies

Bill C-27 Timeline

Bill C-27 introduced

June 2022

Bill C-27 - 2d reading (in progress) April13, 2023

Bill C-27 passes into law

????

Necessary regulations

???? + at least 2 years

(late 2025 at the earliest)

Go-slow enforcement period ….

Conclusion

- Canada is still in a ‘wait and see’ period for AI regulation
- If passed, the core of AIDA’s application and obligations remain to be articulated in regulations
- If not passed, other existing models may help in choosing new path
- In the meantime, existing regulatory bodies will work within the scope of their mandates to address AI issues
- Organizations can prepare by attending to emerging standards for AI governance
- Provinces will need to act to address governance of provincial public sector AI

Questions?

Thank you!

Tscassa@uottawa.ca

www.teresascassa.ca

Twitter: @TeresaScassa