REGULATING AI IN CANADA: A CRITICAL LOOK AT THE PROPOSED *ARTIFICIAL INTELLIGENCE AND DATA ACT*

Teresa Scassa[*]

Canada's Bill C-27, The Digital Charter Implementation Act, includes a proposed Artificial Intelligence and Data Act (AIDA). If passed, the AIDA would establish a series of obligations regarding the use of anonymized data in AI systems; the design, development and making available for use of AI systems generally; and the design, development and making available for use of high-impact AI systems. The bill is challenging to fully understand, as many of these obligations are left to be fleshed out in regulations, including even the definition of the "high impact" AI, to which the AIDA will apply. Oversight of the regime will be the responsibility of the Minister of Industry, who is also responsible for supporting the growth of the AI industry in Canada.

This paper analyzes the AIDA and the context into which it was introduced. This context includes a rapidly evolving AI landscape, as well as important governance initiatives emerging internationally, including from the European Union and the United States. It also explores a set of constraints on Canadian law and policy developments in this space. Part 2 considers how the AIDA is meant to be both 'agile' and a form of risk regulation, and it measures the AIDA against these concepts. In Part 3, the paper considers the scope of the AIDA and a few of the particular constraints that shaped it. These include: the cross-sectoral nature of AI technology, Canada's constitutional division of powers, and the Canadian tendency to

address public and private sector actors separately. Together, the two parts of the paper provide a view of the context and constraints that have shaped the AIDA, casting light on some of the challenges faced in regulating AI, and surfacing important issues for the consultation and engagement that is necessary to properly regulate AI in Canada.

———————————

Le projet de loi C-27, Loi sur la mise en œuvre de la Charte du numérique, comprend la Loi sur l'intelligence artificielle et les données (LIAD) proposée. En cas d'adoption, cette loi établira une série d'obligations concernant l'utilisation de données anonymisées dans les systèmes d'IA; la conception, l'élaboration et le déploiement de systèmes d'IA en général; et la conception, l'élaboration et le déploiement de systèmes d'IA à incidence élevée. Le projet de loi est difficile à comprendre dans son intégralité, car bon nombre de ces obligations doivent être précisées par voie réglementaire, y compris la définition de l'IA « à incidence élevée », à laquelle la LIAD s'appliquera. La supervision du régime incombera au ministre de l'Industrie, qui est également chargé de soutenir la croissance de l'industrie de l'IA au Canada.

L'auteure analyse la LIAD et le contexte dans lequel elle a été déposée. Ce contexte comprend un monde d'IA en évolution rapide, ainsi que d'importantes initiatives de gouvernance émergeant sur le plan international, notamment de l'Union européenne et des États-Unis. Elle couvre également une série de contraintes sur l'évolution du droit et des politiques au Canada dans ce domaine. Dans la deuxième partie, elle examine comment la LIAD est censée être à la fois « agile » et une forme de réglementation de risques, et évalue cette loi par rapport à ces concepts. Dans la troisième partie, l'auteure considère le champ d'application de la LIAD et quelques-unes des contraintes particulières qui l'ont façonnée. Il s'agit notamment de la nature intersectorielle de la technologie de l'IA, de la répartition des pouvoirs au Canada à valeur constitutionnelle, et de la tendance du Canada à traiter séparément les acteurs du secteur public et ceux du secteur privé. Ensemble, les deux parties du document donnent un aperçu du contexte et des contraintes qui ont façonné la LIAD, mettent en lumière certains des défis posés par la réglementation de l'IA et font ressortir des questions importantes pour la consultation et l'engagement qui sont nécessaires pour réglementer correctement l'IA au Canada.

———————————

Contents

1. Introduction

On June 16, 2022, Canada's federal government introduced Bill C-27,[1] *The Digital Charter Implementation Act*, a bill that includes the texts of three separate statutes linked together by commitments in its 2020 Digital Charter.[2] Two of the draft statutes had been part of the earlier Bill C-11,[3] which died on the order paper prior to a federal election in the fall of 2021. The first of these—the *Consumer Privacy Protection Act*—was the long-awaited bill to reform Canada's private sector data protection law.[4] The

---

[1]   Bill C-27, *An Act to enact the Consumer Privacy Protection Act, the Personal Information and Data Protection Tribunal Act and the Artificial Intelligence and Data Act and to make consequential and related amendments to other Acts*, 1st Sess, 44th Parl, 2022 (first reading 16 June 2022), online: <www.parl.ca/DocumentViewer/en/44-1/bill/C-27/first-reading> [perma.cc/QE5C-YW6W] [Bill C-27]. Note that the short title of Bill C-27 is *Digital Charter Implementation Act, 2022*. Bill C-27 consist of the *Consumer Privacy Protection Act* [*CPPA*], *Personal Information and Data Protection Tribunal Act*, and *Artificial Intelligence and Data Act* [*AIDA*].

[2]   Innovation, Science and Economic Development Canada, "Canada's Digital Charter" (last modified 13 March 2023), online: *Government of Canada* <ised-isde.canada.ca/site/innovation-better-canada/en/canadas-digital-charter-trust-digital-world> [perma.cc/XAZ5-ERDV].

[3]   Bill C-11, *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*, 2nd Sess, 43rd Parl, 2020 (first reading 17 November 2020), online: <www.parl.ca/DocumentViewer/en/43-2/bill/C-11/first-reading> [perma.cc/5N3E-UWGW].

[4]   The current data protection law is the *Personal Information Protection and Electronic Documents Act*, SC 2000, c 5 [*PIPEDA*]. There have been numerous and repeated calls for reform of *PIPEDA* from privacy commissioners and others. See e.g. House of Commons, *Towards Privacy by Design: Review of the Personal Information Protection and Electronic Documents Act*, Report of the Standing Committee on Access to Information, Privacy and Ethics, (February 2018) at 30 (Chair: Bob Zimmer), online: <publications.gc.ca/collections/collection_2018/parl/xc73-1/XC73-1-1-421-12-eng.pdf> [perma.cc/Q2JV-HADY]; Office of the Privacy Commissioner of Canada, "The Case for Reforming the *Personal Information Protection and Electronic Documents Act*" (May 2013), online:

second—the *Personal Information and Data Protection Tribunal Act*—created a new adjudicative layer for proceedings under the *CPPA*. The third draft law added to the mix in Bill C-27 came as a surprise to many. The proposed *AIDA* had not been the subject of prior public discussion or consultation.[5] Although the Minister of Innovation, Science and Industry's December 2021 mandate letter mentioned introducing legislation "to advance the Digital Charter," the emphasis was placed on data protection and fair competition in the online marketplace.[6] The only specific mention of AI in the mandate letter relates to "advancing standards and continuing to lead international efforts around coordination, to support artificial intelligence innovations and research in Canada."[7]

The *AIDA* is a relatively brief statute which sets out a series of obligations relating to 1) the use of anonymized data in AI systems, 2) the design, development and making available for use of AI systems generally, and 3) the design, development and making available for use of high-impact AI systems. The brevity is in large part due to a substantial number of important elements being left to regulations. The core focus of the legislation is on high-impact AI systems, although the crucial term "high impact" is not defined.[8] The *AIDA* places evaluation, monitoring and record-keeping obligations on those responsible for AI systems,

---

<www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/pipeda_r/pipeda_r_201305/> [perma.cc/PBK8-SKVA]; Office of the Privacy Commissioner of Canada, "Privacy Law Reform—A Pathway to Respecting Rights and Restoring Trust in Government and the Digital Economy: 2018–2019 Annual Report to Parliament on the *Privacy Act and the Personal Information Protection and Electronic Documents Act*" (2019), online: <www.priv.gc.ca/en/opc-actions-and-decisions/ar_index/201819/ar_201819/> [perma.cc/U7VL-MM7F].

5   The lack of consultation is a major problem with the *AIDA*, *supra* note 1. An interesting point of comparison is with the process that led up to the enactment of *PIPEDA*, *supra* note 4. There, the statute adopted as its normative core, the CSA Model Code, which was the result of a multi-stakeholder consultative process. The *PIPEDA* itself provided for an ombuds model of oversight and regulation, see the discussion of the process for the development of the Model Code in Stephanie Perrin et al, *The Personal Information Protection and Electronic Documents Act: An Annotated Guide,* (Toronto: Irwin Law, 2001) at 15. Although *PIPEDA* later came to be criticized for its lack of real teeth (leading to the enhancement of oversight and enforcement powers in the *CPPA*, *supra* note 1) these have come as a part of the general evolution of regulation and governance in this area.

6   Office of the Prime Minister, *Minister of Innovation, Science and Industry Mandate Letter*, (16 December 2021) (Hon Justin Trudeau), online: <pm.gc.ca/en/mandate-letters/2021/12/16/minister-innovation-science-and-industry-mandate-letter> [perma.cc/E2NU-PWNM] [Mandate Letter].

7   *Ibid*.

8   Under clause 36(b) of the *AIDA*, *supra* note 1, the Governor in Council may make regulations "establishing criteria for the purpose of the definition [sic] *high-impact system* in subsection 5(1)".

with oversight by the Minister of Innovation, Science and Industry (the Minister). The Minister has the power to order those responsible for AI systems to carry out certain duties or to cease using a high impact system in certain circumstances, and these orders are enforceable. Where there is a significant breakdown in meeting obligations under the legislation, a person responsible for an AI system can be subject either to substantial Administrative Monetary Penalties (AMPs) or can be prosecuted for offences under the *AIDA*.

This paper analyzes the *AIDA* and the context into which it was introduced. The goal is not to engage in a detailed analysis or interpretation of the various provisions of the *AIDA*, although some discussion of particular provisions is inevitable. Rather, this paper offers a critical look at some of the factors that have shaped both the form and substance of the *AIDA*, with a view to better understanding its defects and constraints. Part 2 of this paper considers how the *AIDA* is meant to be both 'agile' and a form of risk regulation, and it explores the significance of both of these concepts. In Part 3, the paper considers the scope of Bill C-27 and the constraints that shaped it. These include the cross-sectoral nature of AI technology, Canada's constitutional division of powers, and the tendency to address public and private sector actors separately. These two parts of the paper together provide a view of the context and constraints that have shaped the *AIDA*, casting light on the challenges faced in regulating AI in Canada, and surfacing important issues for the consultation and engagement that is necessary to properly develop AI regulation. The paper concludes with a recommendation that Canada should scrap the *AIDA* and initiate a proper consultation on AI regulation.

2. Regulatory Approach

This part of the paper considers the approach taken to regulating AI in the *AIDA*. As the government uses the term "agile" in the preamble to Bill C-27, the first part of this section considers what constitutes agile regulation.[9] The *AIDA* is also a form of risk regulation, which is the subject of the second part of this section.

A) Agile Regulation

'Agile' is a tech sector buzzword that originated in the context of software development and later spread to the broader management context. The origins of the agile movement in software development are found in the "Agile Manifesto", which sets out these core principles: "[i]ndividuals and interactions over processes and tools; [w]orking software over

---

9   Bill C-27, *supra* note 1, Preamble.

comprehensive documentation; [c]ustomer collaboration over contract negotiation; [r]esponding to change over following a plan."[10] The essence of the agile movement in software has been summarized as entailing the "ability to rapidly and flexibly create and respond to change in the business and technical domains."[11] In the business context, agility has been described as involving "new values, principles, practices, and benefits [that] are a radical alternative to command-and-control-style management."[12] 'Agile' is an ideology that embraces fundamental organizational change: "the Agile organization is a growing, learning, adapting living organism that is in constant flux to exploit new opportunities and add new value for customers."[13] Perhaps unsurprisingly, a concept that has generated so much hype in the software development and business context has migrated to the law and policy context, with agile regulation becoming a buzzword for regulation that can keep pace with a rapidly changing technological innovation context.[14] The 'agile' aspirations of the *AIDA* are explicitly signaled in the preamble to Bill C-27, which states that "organizations of all sizes operate in the digital and data-driven economy and *an agile regulatory framework is necessary* to facilitate compliance with rules by, and promote innovation within, those organizations."[15]

In a report on agile regulation, the World Economic Forum identifies the novel governance challenges which have created a demand for agile regulation.[16] These include the pace of innovation, as well as the difficulty that regulators face in assigning the responsibility for risk management "to different actors in dynamic and complex environments."[17] A further agility challenge is to "respond to innovations whose implications lie partly outside their sectoral or geographical jurisdiction."[18]

---

[10]   Kent Beck et al, "Manifesto for Agile Software Development" (2001), online: *Agile Manifesto* <agilemanifesto.org/> [perma.cc/6PR2-8WYK].

[11]   Torgeir Dingsøyr et al, "A decade of agile methodologies: Towards explaining agile software development" (2012) 85:6 J of Systems and Software 1213 at 1214, DOI: <doi.org/10.1016/j.jss.2012.02.033> [perma.cc/HM2Z-U2AM].

[12]   Darrell Rigby, Jeff Sutherland & Hirotaka Takeuchi, "Embracing Agile" (May 2016), online: *Harvard Business Review* <hbr.org/2016/05/embracing-agile> [perma. cc/3EMK-LLTQ].

[13]   Steve Denning, "What is Agile?" (13 August 2016), online: *Forbes* <www.forbes. com/sites/stevedenning/2016/08/13/what-is-agile/?sh=7394c8df26e3> [perma.cc/D926-X2VZ].

[14]   World Economic Forum, "Agile Regulation for the Fourth Industrial Revolution: A Toolkit for Regulators" (December 2020), online (pdf): <www3.weforum.org/docs/ WEF_Agile_Regulation_for_the_Fourth_Industrial_Revolution_2020.pdf> [perma.cc/7F DB-7CZ9] [WEF].

[15]   Bill C-27, *supra* note 1, Preamble [emphasis added].

[16]   WEF, *supra* note 14.

[17]   *Ibid* at 6.

[18]   *Ibid.*

The Canadian government's approach to agility in the *AIDA* is manifested in two main ways. First, many of the core terms and obligations are left to be defined in regulations. Second, oversight and governance of the legal obligations remains within the Minister's office; no new or independent regulatory body is created for AI, nor is responsibility assigned to an existing regulator. Yet, as I will argue below, agile regulation is not about drafting laws that can, in theory, be more easily changed by relying on regulations instead of statutory provisions. Rather, it is about supporting regulators to engage in more flexible, responsive, and data-driven regulatory practices.

1) Regulations

The WEF characterizes agile regulation as "anticipatory," but cautions that "[f]oresight should not be used as a rush to regulate."[19] It suggests that agile regulation involves "a cycle of continuous learning and adaptation as the technology develops,"[20] and thus favours soft law in the form of non-binding guidance, standards and codes of practice.[21] The US National Institute of Standards and Technology Risk Management Framework would be an example of this.[22] The *AIDA* provides for Ministerial guidance,[23] but codes of practice are not addressed in the bill.[24] Standards are not specifically addressed, although the plan may be for standards to be adopted by regulation. It is a striking feature of the *AIDA* that so much is left to be defined or set out in regulations, with both the Minister and the Governor-in-Council having regulation-making powers. Under the *AIDA*, organizations are required to keep records of how they manage anonymized data,[25] how they assess whether their AI system is high risk,[26] how they have established measures to "identify, assess and mitigate the risk of harm and biased output that could result from the use of the system,"[27] and how they monitor compliance with the mitigation

---

19   *Ibid* at 11.
20   *Ibid*.
21   *Ibid* at 17. A strong example of this is the Risk Management Framework developed by the National Institute for Standards and Technology (NIST) in the United States. See: National Institute of Standards and Technology, "Artificial Intelligence Risk Management Framework (AI RMF 1.0)" (January 2023), online (pdf): <www.nist.gov/itl/ai-risk-management-framework> [perma.cc/SCP2-F6YC] [NIST Framework].
22   NIST Framework, *supra* note 21.
23   *AIDA*, *supra* note 1, cl 32(c).
24   The adoption of Codes of Practice is provided for in the *CPPA* which is also part of Bill C-27, but are not provided for in the *AIDA*.
25   *AIDA*, *supra* note 1, cl 10(1)(a).
26   *Ibid*, cl 10(1)(b).
27   *Ibid*, cl 8.

measures.[28] The details of these record-keeping requirements are left to be fleshed out in regulations that are the responsibility of the Minister.[29] The Minister is also empowered to make regulations regarding "the time and the manner" in which organizations must publish descriptions of their AI systems under clause 11 of the *AIDA*; these regulations may also specify the information that should be included in the description.[30] The Minister is responsible for regulations relating to the publication of any information that the Minister orders to be published under clause 18, and regarding the requirements to give notice[31] under clause 12 of when an AI system is judged by the person responsible to have resulted in or be likely to result in material harm.

The Governor-in-Council has even more substantial regulation-making powers. It is the Governor-in-Council that is left to define what constitutes a "high impact system";[32] it is also responsible for setting out how a person responsible should assess whether an AI system is "high impact."[33] The Governor-in-Council must establish regulations about how a person responsible should establish measures to mitigate the harms from high impact systems, and to monitor high impact systems.[34] The Governor-in-Council is responsible for establishing measures for the anonymization of data.[35] It must specify the criteria for determining if a system results or is likely to result in material harm.[36] The Governor-in-Council is charged with setting out the qualifications for auditors of systems and for determining how certain information about a system should be published.[37] The Governor-in-Council may add to the list of persons to whom the *AIDA* does not apply under clause 3(2)(d).[38] It may also add to the list of regulators to whom the Minister may disclose information under clause 26(1)(f).[39]

The Governor-in-Council is also responsible for enacting regulations regarding AMPs under the *AIDA*. Specifically, the Governor-in-Council will designate the contravention of which provisions will constitute a

---

28   *Ibid*, cl 9, 10(2).
29   *Ibid*, cl 37(a).
30   *Ibid*, cl 37(b).
31   *Ibid*, cl 37(c).
32   *Ibid*, cl 36(b).
33   *Ibid*, cl 36(d).
34   *Ibid*, cl 36(c).
35   *Ibid*.
36   *Ibid*, cl 36(e).
37   *Ibid*, cl 18(2).
38   *Ibid*, cl 3(3).
39   *Ibid*, cl 36(g).

violation for which AMPs may be assessed.[40] It is also responsible for determining whether violations will be classified as "minor," "serious" or "very serious."[41] The Governor-in-Council may determine when a violation is a separate violation on each day it takes place.[42] How proceedings for violations will unfold will be set out in regulations enacted by the Governor-in-Council.[43] The Governor-in-Council will also enact regulations to set guidelines for the amount or range of AMPs depending upon designated classes of persons, the factors to be taken into account in setting AMPs, how AMPs are to be paid or recovered, any reviews or appeals, and compliance agreements.[44] The bulk of the AMPs framework, in substance and procedure, is thus left for regulations. All that the *AIDA* really tells us about these AMPs is that their purpose is "to promote compliance with this Part and not to punish."[45]

In some instances, the reliance upon regulations in the *AIDA* appears intended to enable the incorporation of standards into certain regulations. Michel Girard, in arguing for standards in the high-technology sector notes:

> Standards cover a wide spectrum of subjects, from definitions, ontology classifications, metrics, measurement, manufacturing techniques and processes to delivery systems and beyond. They set out requirements, specifications, guidelines or model characteristics that can be consistently applied to ensure that products, materials, processes, systems and services perform as intended—qualitatively, safely and efficiently.[46]

The federal government has been very much involved in supporting the development of standards in the data and technology sectors. The 2021 Federal budget, for example, contained funding to support the work of standards development in this area.[47] The development of standards can

---

40   *Ibid*, cl 29(4)(a).
41   *Ibid*, cl 29(4)(b).
42   *Ibid*, cl 29(4)(a).
43   *Ibid*, cl 29(4)(c).
44   *Ibid*, cl 29(4)(d).
45   *Ibid*, cl 29(2).
46   Michel Girard, "Big Data Analytics Need Standards to Thrive: What Standards Are and Why They Matter" (January 2019) at 3, online (pdf): *Centre for International Governance Innovation* <www.cigionline.org/static/documents/documents/Paper%20no.209.pdf> [perma.cc/A5FQ-AMD5].
47   The budget provided for "$8.6 million over five years, starting in 2021–22, to advance the development and adoption of standards related to artificial intelligence" (Department of Finance Canada, "Creating Jobs and Growth" (last modified 19 April 2021) at 4.6, online: *Government of Canada* <www.budget.gc.ca/2021/report-rapport/p2-en.html> [perma.cc/8AQL-A4YV] [Budget]).

be multi-party and multi-sectoral, and thus can approximate a consultative process for regulation-making, although it is not evident that civil society or the broader public has a seat at the standards table.[48] Standards can be developed locally or internationally; at the international level, there has been competition to see who will set global standards for AI and its related technologies.[49] In Canada, the Digital Governance Council (formerly the CIO Strategy Council) has been active in the development of technology-related standards.[50] A government led initiative under the Standards Council of Canada, the Data Governance Standardization Collaborative[51] has also been active in developing standards for various use cases. Its initial report indicates that governments should consider incorporation by reference in regulations of any standards developed through this process.[52] Under the *AIDA*, standards could be adopted by regulation for things such as the anonymization of data, the qualifications of auditors, and possibly even risk assessment. It is also possible to create a standard for evaluating things like bias and discrimination,[53] although one would expect any such process to be more participatory and representative of

---

48   The *PIPEDA* incorporated the CSA Model Code for the Protection of Personal Information, taking advantage of the consensus-based approach to the development of the Code (Michael Deturbide & Teresa Scassa, *Digital Commerce in Canada* (Toronto: LexisNexis, 2020) at 108).

49   Girard proposes an alternate, more multi-party route for international standards development. See Michel Girard, "Data Standards Task Force for Digital Cooperation" (August 2020), online (pdf): *Centre for International Governance Innovation* <www.cigionline.org/static/documents/documents/PB%20no.162.pdf> [perma.cc/Z8CD-PUWR].

50   The Digital Governance Council's website describes it as "Canada's only national body for delivering a coordinated national approach to digital governance" (Digital Governance Council, "Powering Trust in Canada's Digital Economy" (2023), online: <dgc-cgn.org//> [perma.cc/84DX-AABV]). Its list of members identifies organizations that are predominantly large private sector companies, but which also include some federal government departments and the City of Toronto (Digital Governance Council, "About the Digital Governance Council" (2023), online: <dgc-cgn.org/about/> [perma.cc/V6DJ-BJ56]).

51   Standards Council of Canada, "Canadian Data Governance Standardization Collaborative" (2023), online: <www.scc.ca/en/flagships/data-governance> [perma.cc/6F52-YZBU].

52   Standards Council of Canada, "Canadian Data Governance Standardization Roadmap" at 3, online (pdf): <www.scc.ca/en/system/files/publications/SCC_Data_Gov_Roadmap_EN.pdf> [perma.cc/39C6-MYVS] [Roadmap].

53   See Natalie Heisler, *Standards for the control of algorithmic bias in the Canadian administrative context* (Master Thesis, University of Waterloo, 2022) <uwspace.uwaterloo.ca/bitstream/handle/10012/18677/Heisler_Natalie.pdf?sequence=5&isAllowed=y> [perma.cc/GQ9T-WLTX].

diverse communities than what currently takes place at the standards tables.[54]

2) Roles

Another feature of agile regulation is that in most cases there is an actual regulator who can adopt different strategies or tools to enable a more agile regulatory approach. Regulators in the financial sector,[55] in data protection,[56] or in the health sector,[57] for example, have created regulatory sandboxes that allow them to experiment and develop more agile regulatory approaches. The *AIDA* does not confer powers on an established regulator. Instead, it sets up the Minister as the actor responsible for oversight and enforcement, but the Minister may delegate any or all of his or her oversight powers to a new Artificial Intelligence and Data Commissioner, a role created by clause 33.[58] While other federal Commissioners have their own agencies and statutory powers, the Data Commissioner is described in the *AIDA* as "a senior official of the department over which the Minister presides."[59] Thus, he or she has no independence, and will

---

54   The Canadian Data Governance Standardization Collaborative describes its membership as constituting "a community of more than 220 Canadian stakeholders from industry, governments, civil society, academia and Standards Development Organizations (SDOs)" (Roadmap, *supra* note 52 at 5). A list of the collaborative's membership is found in Annex E of Roadmap, *supra* note 52.

55   See, for example, the sandbox created by the Canadian Securities Administrators, "CSA Regulatory Sandbox" (2023), online: <www.securities-administrators.ca/resources/regulatory-sandbox/> [perma.cc/9ATE-HMVU] [CSA Regulatory Sandbox].

56   The Information Commissioner's Office in the UK has launched a privacy regulatory sandbox, "Regulatory Sandbox", online: *Information Commissioner's Office* <ico.org.uk/for-organisations/regulatory-sandbox/> [perma.cc/8SCA-69VZ].

57   Marianne Apostolides, "Health Canada's controversial 'regulatory sandbox': Enabling innovation or lowering the bar for safety?" (4 November 2017), online: *healthydebate* <healthydebate.ca/2021/11/topic/health-canadas-regulatory-sandbox/> [perma.cc/8L33-QT6P].

58   *AIDA*, *supra* note 1, cl 33. The role of Data Commissioner was first floated in the 2019 Mandate Letter to the Minister of Industry, which provided that the Minister would: "[w]ith the support of the Minister of Canadian Heritage, create new regulations for large digital companies to better protect people's personal data and encourage greater competition in the digital marketplace. A newly created Data Commissioner will oversee those regulations" (Office of the Prime Minister, Archived—Minister of Innovation, Science and Industry Mandate Letter, (13 December 2019) (Hon Justin Trudeau), online: <pm.gc.ca/en/mandate-letters/2019/12/13/archived-minister-innovation-science-and-industry-mandate-letter> [perma.cc/D8YT-3BAV]). The 2021 Federal Budget provided funding for the Data Commissioner. The budget referred to the role of the Data Commissioner as to "inform government and business approaches to data-driven issues to help protect people's personal data and to encourage innovation in the digital marketplace" (Budget, *supra* note 47 at 4.7).

59   *AIDA*, *supra* note 1, cl 33(1).

lack security of tenure in their role as Commissioner, which is essentially "to assist the Minister."[60] Both the Minister and the Data Commissioner are located within the department charged with supporting innovation and economic development, which should also raise questions regarding independence, particularly given the powers granted under the *AIDA* to both make and enforce policy.[61]

To perhaps add a gloss of independent input into the administration of the statute, the *AIDA* provides for the creation of an advisory committee (clause 35(1)) that will offer the Minister "advice on any matters related to this Part."[62] However, neither the *AIDA* nor its anticipated regulations will provide for any particular composition of the advisory committee, for the appointment of a chair with a fixed term, or for any reports by the committee on its advice or activities. It is the Minister who may choose to publish advice he or she receives from the committee on a publicly available website (clause 35(2)).[63]

---

60   *Ibid.*

61   *Ibid*, cl 35(1). See Mardi Witzel, "A Few Questions about Canada's Artificial Intelligence and Data Act" (11 August 2022), online: *Centre for International Governance Innovation* <www.cigionline.org/articles/a-few-questions-about-canadas-artificial-intelligence-and-data-act/> [perma.cc/9KSP-2KWC]. Although substantial AMPs may be levied under the *AIDA*, it is unknown who will make the decision to levy AMPs, nor do we know what procedural safeguards will be in place, or how reviews or appeals will be conducted (or by whom). The *AIDA* empowers the Governor in Council to make regulations "respecting the persons or classes of persons who may exercise any power or perform any duty or function in relation to the scheme," so this too is left for regulations (*supra* note 1, cl 29(4)(g)).

62   In its report on agile regulation, the WEF, *supra* note 14 at 10, notes that advisory panels are increasingly used "to advise regulators on the impacts of technological innovation and the resulting need for reform." Although advisory panels can create an impression on inclusive consultation, Vural, Herder & Graham observe that in the Canadian health sector, advisory committees appointed by government and largely populated by private sector actors have been used to play role in the policy process (Ipek Eren Vural, Matthew Herder & Janice E Graham, "From sandbox to pandemic: Agile reform of Canadian drug regulation" (2021) 125:9 Health Policy 1115 at 1117, DOI: <doi.org/10.1016/j.healthpol.2021.04.018> [perma.cc/L96Y-BQUN]). Canada already has an AI Advisory Council, although members serve on a volunteer basis. Created in 2019, the Council "advises the Government of Canada on building Canada's strengths and global leadership in AI, identifying opportunities to create economic growth that benefits all Canadians, and ensuring that AI advancements reflect Canadian values" (Innovation, Science and Economic Development Canada, "Advisory Council on Artificial Intelligence" (last modified 26 April 2022), online: *Government of Canada* <ised-isde.canada.ca/site/advisory-council-artificial-intelligence/en> [perma.cc/82DF-HBB7]). Interestingly, the mandate of this version of the council does not include providing advice on AI regulation and governance.

63   *AIDA*, *supra* note 1, cl 35(2).

3) Summary

Agile regulation is about systemic change and adaptation, and is premised on feedback loops that enable learning and responsiveness. 'Agility' does not require the formlessness evident in the *AIDA*. As the WEF notes, "[a] more rigid regulatory framework need not necessarily be a barrier to agility."[64] Different tools and techniques adopted by regulators can provide necessary agility,[65] although these are often dependent upon the existence of an actual regulatory body—something that is absent from the *AIDA*.[66] AI governance at its best will involve experimenting, measurement, feedback, and adaptation. These features are not evident in the *AIDA*, which simply shifts the responsibility for establishing legal norms from legislation to regulations. Not only is this not agile in any meaningful way, with so much left to regulations there is a risk that the legislation—or key parts of it—will never take effect. There are certainly instances of other federal laws left incomplete by never-drafted regulations. For example, the private right of action provided for in Canada's Anti-Spam Law,[67] cannot

---

64   WEF, *supra* note 14 at 16.

65   Examples of these can include innovation hubs, regulatory sandboxes, and even competitions to support or shape how innovation takes place. On innovation hubs and regulatory sandboxes, see Ross P Buckley et al, "Building Fintech Ecosystems: Regulatory Sandboxes, Innovation Hubs and Beyond" (2020) 61 Wash UJL & Pol'y 55; Oliver R Goodenough & David L Shrier, "Regulatory Sandboxes" in David L Shrier & Alex Pentland, eds, *Global Fintech: Financial Innovation in the Connected World* (Cambridge, MA: MIT Press, 2022) at 203; Lauren Fahy, "Regulator Reputation and Stakeholder Participation: A Case Study of the UK's Regulatory Sandbox for Fintech" (2022) 13:1 European J of Risk Regulation 138; United Nations Secretary-General's Special Advocate for Inclusive Finance for Development & Cambridge Centre for Alternative Finance, "Early Lessons on Regulatory Innovations to Enable Inclusive FinTech: Innovation Offices, Regulatory Sandboxes, and RegTech" (2019), online(pdf): <www.jbs.cam.ac.uk/wp-content/uploads/2020/08/2019-early-lessons-regulatory-innovations-enable-inclusive-fintech.pdf> [perma.cc/4UX3-48BG].

66   Regulatory sandboxes are typically established under the governance of a regulator. For example, the privacy sandbox in the UK is created and overseen by the Information Commissioner. An AI regulatory sandbox established in Norway, is overseen by the Norwegian data protection authority. See "Norwegian DPA creating regulatory sandbox for AI" (27 May 2020), online: *iapp* <iapp.org/news/a/norwegian-dpa-creating-regulatory-sandbox-for-ai/> [perma.cc/99VB-M95K].

67   *An Act to promote the efficiency and adaptability of the Canadian economy by regulating certain activities that discourage reliance on electronic means of carrying out commercial activities, and to amend the Canadian Radio-television and Telecommunications Commission Act, the Competition Act, the Personal Information Protection and Electronic Documents Act and the Telecommunications Act*, SC 2010, c 23 [*CASL*].

come into effect until the necessary regulations are drafted—12 years after the enactment of the law,[68] the regulations remain undrafted.

Agile regulation usually come from a specific regulator and can include techniques such as regulatory sandboxes,[69] innovation hubs,[70] and data-driven evaluations of regulatory impact.[71] In the case of the *AIDA*, there is no established or incumbent regulator who is given a new 'agile' role. Instead, the Minister takes on the role of regulator, with a poorly defined framework, and no separation between the power to make regulations and the power to oversee compliance and enforcement. The point here is that the agile label should not be used to support legislation that leaves everything to regulation, since it specifically refers to a suite of new tools and approaches that can be used by a regulator to improve their responsiveness to rapid technological change.

B) Risk Regulation

The second contextual factor that shapes the *AIDA* is its character as a form of risk regulation. Responsive regulation which takes into account assessments of risk received serious scholarly attention in the early 1990s, and was the subject of a major report to the UK government in 2005.[72] At its core, it proposes that regulators "should focus their efforts on the most serious risks they face in achieving their objectives."[73] The fast-paced technology environment is an obvious candidate for risk regulation, as regulators seek to minimize risks while at the same time facilitating and encouraging ongoing innovation and development. Margot Kaminski observes that risk regulation is well-suited to AI since AI systems are "technologically complex" and "at least in part inscrutable,"[74] which makes

---

[68]   *Ibid*, ss 47–49. Although the law was passed in 2010, it did not come into effect until 2014, and even then, it was phased in. Nevertheless, there has been a long enough wait for regulations regarding the private right of action that it is fair to wonder if this provision will ever be made effective.

[69]   See e.g. Buckley et al, *supra* note 65; Goodenough & Shrier, *supra* note 65.

[70]   See Buckley et al, *supra* note 65.

[71]   WEF, *supra* note 14 at 27–31.

[72]   Ian Ayres & John Braithwaite, *Responsive Regulation: Transcending the Deregulation Debate* (New York: Oxford University Press, 1992); Philip Hampton, "Reducing administrative burdens: effective inspection and enforcement" (March 2005), online (pdf): *HM Treasury* <www.regulation.org.uk/library/2005_hampton_report.pdf> [perma.cc/VM59-29JE].

[73]   Robert Baldwin & Julia Black, "Driving Priorities in Risk-based Regulation: What's the Problem?" (2016) 43:4 JL & Soc'y 565, DOI: <doi.org/10.1111/jols.12003> [perma.cc/XA8T-N2MD].

[74]   Margot E Kaminski, "Regulating the Risks of AI" (2023) at 41 [forthcoming in 103 BUL Rev, 2023] online: <papers.ssrn.com/sol3/papers.cfm?abstract_id=4195066> [perma.cc/MLP9-NQ6T].

ex post remedial approaches challenging. Further, she notes that like any software system, AI systems are likely to fail, making *ex ante* modes of regulation more useful in anticipating and mitigating potential harms.[75]

Kaminski notes that risk-based approaches to the regulation of AI have been adopted in both the EU in the AI Act[76] and the US, with its NIST Framework.[77] She observes that risk regulation involves "both a set of regulatory goals and a set of tools."[78] The goals are generally the reduction or elimination of risk, and Kaminski notes that the risks that attract this form of regulation generally come from "complex systems or technologies."[79] She defines the tools in the risk regulation tool-box as falling into three broad categories: precautionary tactics, risk assessment and mitigation, and post-market and ongoing measures. Importantly, risk regulation is aimed at preventing or mitigating harm, rather than providing redress or compensation.

Kaminski identifies five broad arguments in support of the use of risk regulation for AI systems. The first is that *ex ante* regulation that seeks to reduce risk by shaping the development of technologies may simply be better suited to AI than *ex post* systems that focus on redress and compensation for harm.[80] We already know that there will be significant challenges in litigating harms caused by AI systems. In many cases, it will be difficult to prove causation; the complexity of both algorithms and data, combined with the need to navigate trade secrets and confidential information, mean that litigation will be complex and enormously costly.[81] Risk regulation promises to be more effective by nipping potential harm in the bud, rather than letting complex litigation shape corporate behaviour. Second, Kaminski notes that it may be difficult in some cases to quantify the harms experienced as a result of faulty AI.[82] This may be

---

[75]   *Ibid* at 42.

[76]   *Ibid* at 55. See "Proposal for a Regulation of The European Parliament and of the Council Laying Down Harmonised Rules On Artificial Intelligence (Artificial Intelligence Act) And Amending Certain Union Legislative Acts" (2021), online: *EUR-Lex* <eur-lex. europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52021PC0206> [perma.cc/TXP3-GE 3H] [EU AI Act].

[77]   NIST Framework, *supra* note 21.

[78]   Kaminski, *supra* note 74 at 26.

[79]   *Ibid*.

[80]   For a discussion of this in the context of AI in health care, see Bradley Henderson, Colleen M Flood & Teresa Scassa, "Artificial Intelligence in Canadian Health Care: Will the Law Protect Us from Algorithmic Bias Resulting in Discrimination?" (2021) 19:2 CJLT 475.

[81]   See e.g. Kristen Thomasen, "AI and Tort Law" in Florian Martin-Bariteau & Teresa Scassa, eds, *Artificial Intelligence and the Law in Canada* (Toronto: LexisNexis Canada, 2021) 103 at 117.

[82]   Kaminski, *supra* note 74 at 18.

in part due to causation issues, but it will also be due in some cases to the challenges of quantifying more intangible harms. In Canada, the problem of quantifying intangible harms has emerged, for example, in the context of large, class-action privacy lawsuits, a number of which have failed on the issues of causation and proof of harm.[83] Third, Kaminski notes that *ex ante* regulation can be beneficial because it can shape system design, "addressing harms on a collective level rather than waiting for individuals to invoke their rights."[84] Thus, by anticipating the potential for bias, in theory, systems can be designed to minimize those factors that might result in bias and can also provide for ongoing monitoring to identify problems as they emerge. Kaminski's fourth argument is generally to note that a considerable number of researchers either support risk regulation in this area or support use of tools to govern AI that are clearly part of the risk regulation tool kit.[85] These include licensing, certification and impact assessments.[86] Her final point notes the significant challenges faced overall in regulating a technology that presents so many "unknown unknowns."[87] The risk regulation approach is evident in the EU AI Act, in the NIST Framework in the US,[88] and in Canada's *Directive on Automated Decision-Making*,[89] to provide just a few examples. The *AIDA* also falls into this category.

As is typical with risk regulation, the *AIDA* requires regulated persons to engage in a number of *ex ante* activities designed to reduce the risks of the systems being designed or developed, although in the case of the *AIDA*, as noted above, most of the details of the obligations are left to regulations that have yet to be drafted. Under the *AIDA*, persons responsible for high-impact AI systems have an obligation to identify, assess, and mitigate risks of harm or biased output. Those persons must also notify the Minister "as soon as feasible" if a system for which they are responsible "results or is likely to result in material harm."[90] A number of oversight and enforcement functions are triggered by harm or a risk of harm. For example, if the Minister has reasonable grounds to believe that a system may result in harm or biased output, she or he can demand

83   See e.g. *Del Giudice v Thompson*, 2021 ONSC 5379 at para 224 (on appeal to the Ont CA); *Sofio c Organisme canadien de réglementation du commerce des valeurs mobilières (OCRCVM)*, 2015 QCCA 1820.

84   Kaminski, *supra* note 74 at 19.

85   *Ibid*.

86   *Ibid* at 19–20.

87   *Ibid* at 20.

88   Kaminski, *supra* note 74 at 3; NIST Framework, *supra* note 21.

89   Treasury Board Secretariat, "Directive on Automated Decision-Making" (last modified 28 June 2021), online: *Government of Canada* <www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=32592> [perma.cc/9FPF-EFH9] [DADM].

90   *AIDA*, *supra* note 1, cl 12.

the production of certain records.[91] If there is a serious risk of imminent harm, the Minister may order a person responsible to cease using a high impact system.[92] The Minister is also empowered to make public certain information about a system where she or he believes that there is a serious risk of imminent harm and the publication of the information is essential to preventing it.[93] Elevated levels of harm are also a trigger for the offence in clause 39, which involves "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."[94]

As long as innovators comply with the rules in the *AIDA*, they are free to innovate—unlike the EU AI Act, the bill does not prohibit any technologies.[95] There are some limited public transparency requirements for high impact systems.[96] There is provision for oversight, but it is not proactive compliance—the Minister must have "reasonable grounds to believe" that there has been a contravention before she or he can act.[97] The Minister's powers include requiring an audit (by a third party chosen and paid for by the audited organization) and requiring changes to be made based on the audit. She or he can also order that an organization cease using a high impact system. If orders from the Minister are insufficient to resolve issues, there are two additional and alternate routes for compliance. A finding of a violation of the *AIDA* can lead to the imposition of AMPs or the compliance shortcomings can be treated as an offence leading to prosecution.

Kaminski emphasizes that adopting risk regulation "is neither inevitable nor a neutral tool."[98] She notes, for example, that AI systems are known to produce biased outputs that can cause or contribute to discrimination. Risk regulation attempts to avoid or mitigate such risks. Yet, as Kaminski notes, framing discrimination as a risk suggests that it is something that, although we try to prevent it, is an anticipated outcome of activity in this sector. She observes that "regulating risk often involves society-wide tradeoffs. Even immense individual harms may get dismissed through the lens of risk analysis, in the face of significant collective

---

91   *Ibid*, cl 14.
92   *Ibid*, cl 17(1).
93   *Ibid*, cl 28.
94   *Ibid*, cl 39.
95   The EU AI Act, *supra* note 76, sets out a series of prohibitions in art 5.
96   In addition to these, the Minister can also order additional information to be published under *AIDA*, *supra* note 1, cl 18, but this also falls short of publishing confidential information.
97   *AIDA*, *supra* note 1, cls 14, 15(1).
98   Kaminski, *supra* note 74 at 3.

benefits."[99] In the case of AI and innovation, there is considerable evidence of Canada's enthusiasm for supporting and encouraging the development of the AI sector with a view to the various economic and other benefits that will ensue.[100] In fact, the mandate of the Ministry charged with oversight of the *AIDA* is to "[a]dvance the Pan-Canadian Artificial Intelligence Strategy and additional measures, such as advancing standards and continuing to lead international efforts around coordination, to support artificial intelligence innovations and research in Canada."[101] The *AIDA*, which seeks to mitigate harm to individuals and biased output, therefore signals an acceptance that these will be important costs of encouraging innovation. The goal is to identify and mitigate the harms to the extent possible, but they are clearly acceptable costs—up to the point of the as yet undefined 'high impact'.[102] It is worth noting that the EU AI Act refers to high-*risk* systems. The NIST Framework refers to levels of risk as well, noting that the risks can lead to different kinds and levels of impact.

Robert Baldwin and Julia Black observe that risk regulation first requires the identification and framing of risk. They note that "the way [a risk] is construed will shape the manner in which it is then assessed and managed."[103] They observe that how risks are framed is influenced by "*theoretical* or *ideological* perspectives; *operational and resourcing* factors; and *political communicative* and *reputational* pressures."[104] The core risks to be regulated by the *AIDA* appear to be bias (defined as discriminatory bias) and harm. Harm and bias are identified as risks but are framed in terms of individual and quantifiable harm,[105] reflecting a distinct ideological perspective that eschews the more complex framing of group or collective harms and systemic discrimination. The federal government's own DADM (another example of risk regulation) does a better job of addressing collective harms than does the *AIDA*. In assessing the potential impact of an automated decision systems (ADS), the DADM

---

99   *Ibid* at 8.

100   See e.g. Council of Canadian Academies, "Leaps and Boundaries: The Expert Panel on Artificial Intelligence for Science and Engineering" (2022) at 16–20, online (pdf): <cca-reports.ca/wp-content/uploads/2022/05/Leaps-and-Boundaries_FINAL-DIGITAL. pdf> [perma.cc/W8QE-JXGS].

101   Mandate Letter, *supra* note 6.

102   This is in contrast to the EU AI Act, *supra* note 76, which has already (to some controversy) identified areas where societal risks are simply too great, imposing outright bans on certain types of AI systems.

103   Baldwin & Black, *supra* note 73 at 569.

104   *Ibid* at 570 [emphasis in original].

105   The definition of 'harm' in the *AIDA*, *supra* note 1 focuses on harms to individuals rather than collective harms or harms to both individuals and/or collectives. Harm is defined in cl 5(1) to mean "(a) physical or psychological harm to an individual; (b) damage to an individual's property; or (c) economic loss to an individual".

takes into account: "the rights of individuals or communities," "the health or well-being of individuals or communities," "the economic interests of individuals, entities, or communities," and "the ongoing sustainability of an ecosystem."[106] Similarly, the NIST Framework considers potential impacts on "individuals, groups, communities, organizations, society, the environment, and the planet."[107]

In addition, the preoccupation of the *AIDA* seems to be with only a limited range of data-related issues. Baldwin and Black suggest that "[r]egulators who are concerned to sustain support for their actions will tend to categorize risks in ways that respond to public (or group or industry) perceptions of risk and their respective expectations of the regulator."[108] By setting an early agenda for regulation in the Digital Charter, the government conditioned public expectations. This in turn shapes how the risks regulated by the *AIDA* are both identified and addressed. Regulations under the *AIDA* will set out how data should be anonymized and governed, suggesting that requirements exist only for anonymized personal data. The focus is also on reidentification risk and bias; no obligations are imposed regarding ensuring that data, whether human-derived or otherwise, are fit for purpose or of sufficient quality.[109]

Kaminski notes that "risk regulation works best on quantifiable problems,"[110] and she gives the example of setting rules for the maximum quantity of a chemical to be released into the environment. This is much harder to do in the context of AI, because many of the harms will be difficult to quantify. The *AIDA* focuses on quantifiable harms to individuals or their property. Yet in doing so, it runs the serious risk of doing what Kaminski refers to as rendering "other harder-to-measure harms invisible."[111] As noted earlier, by defining high-risk AI systems in terms of their impacts on *individuals*, the law appears to exclude (or at least overlook) groups and communities. It also very significantly focuses on what are typically considered quantifiable harms, and uses language that suggests quantifiability (economic loss, damage to property, physical or psychological harm). As Kaminski notes, the challenge of quantifying harms is one reason to adopt risk regulation; it seems odd, then, to

---

[106]   DADM, *supra* note 89 at Appendix B.

[107]   NIST Framework, *supra* note 21 at 4.

[108]   Baldwin & Black, *supra* note 73 at 579.

[109]   Separate obligations under the *AIDA* exist for AI systems; even then, the focus is only on discriminatory bias. For an explanation of the different kinds of bias, see Henderson, Flood & Scassa, *supra* note 80 at 480–85.

[110]   Kaminski, *supra* note 74 at 32.

[111]   *Ibid* at 33.

emphasize quantification in defining harm.[112] Where an ADS results in racially biased outcomes, there may be real individual harms (such as, for example, the loss of employment), but the collective harms are every bit as important, although some of them may be difficult to quantify (such as continued poverty, alienation, and disenfranchisement). Further, it may be difficult to prove causation with individual harm; some biases in algorithms may be more evident when assessed in terms of collective impact. Like the EU AI Act, the *AIDA* does not provide for actionable rights for individuals. This is because its focus is risk regulation. *Ex post* recourses and remedies may exist separately. These can include recourse in tort law, claims for breach of contract, or recourse under statutes such as *PIPEDA*, although the extent to which these recourses are adapted to the challenges of litigating AI harms remains to be seen. Similarly, the *AIDA* does not provide for the filing or investigation of complaints by individuals or groups regarding any harms they may believe they have suffered, even though harm to *individuals* (but not groups or communities) is a trigger for certain consequences under the *AIDA*. In extreme cases, those consequences could include the imposition of AMPs or prosecution.

Choosing a risk-regulation approach has shaped the normative framework of the *AIDA*, creating a focus on *ex ante* measures designed to anticipate and mitigate risks and harms. AI is likely a subject matter well-suited to a risk-regulation approach. However, the approach to risk regulation in the *AIDA* is also influenced by ideological and political tendencies. These are latent in the almost complete lack of public consultation on this bill, the apparent intention to adopt industry-led standards in the regulations, and even in the tabling of a bill in Parliament that is so devoid of substantive content that it is almost a regulatory blank cheque. It is particularly evident in the location of governance and oversight of the *AIDA* squarely in the Ministry that is also charged with supporting the Canadian AI industry. It is also apparent in some of the choices made in the identification of risks (quantifiable and individual) and the *AIDA*'s limitation of data-related governance to discriminatory bias and reidentification risk in relation to human-derived data.

---

112   For example, a growing number of class action lawsuits relating to significant data breaches are failing because of the impossibility of proving material loss either because, although thousands may have been impacted, the individual losses are impossible to quantify, or because it is impossible to prove a causal link between very real identity theft and that particular data breach, see Nicolas Vermeys, "Why Class Action Suits for Security Breaches Need to Look Beyond Privacy Concerns" in Ignacio N Cofone, ed, *Class Actions in Privacy Law* (London: Routledge Taylor & Francis Group, 2022) 81 at 94–96.

3. Structural Constraints

Existing constraints within any jurisdiction will necessarily shape the regulation of technology and/or technological harms. For lack of a better term, I group these under the label 'structural constraints.' Structural constraints take on added significance in the case of emerging and rapidly developing technologies. They may impact the speed at which regulation can evolve, and the comprehensiveness of that regulation. In this section, I identify three broad structural constraints that have shaped the *AIDA*. The first is the way in which existing and established laws/institutions impact the regulation of new technologies. The second is the impact of the constitutional division of powers in a federal state such as Canada. The third is the distinction between public and private sectors when it comes to regulation.

A) Subject Matter

The *AIDA* is designed to regulate 'high impact' AI. However, unlike other subject matter for regulation, AI cuts across all sectors of the economy.[113] As a result, its regulation may impact technologies already regulated by other actors, creating the potential for overlap. Further, as AI impacts other sectors of the economy, the *AIDA* may conflict or overlap with norms or rules in other legislation such as data protection laws, as well as emerging laws for issues such as platform governance.[114] Government departments and agencies have already been experimenting with different forms of AI governance related to their mandates. For example, Health Canada is in the process of establishing a regulatory sandbox for Advance Therapeutic Products,[115] the Canadian Securities Administrators have developed a regulatory sandbox for fintech innovation,[116] and Transport Canada has

---

[113]   NIST Framework, *supra* note 21. Bogucki et al refer to this as part of AI's "cross-cutting nature," and observe that this "creates the risk of inconsistencies and overlaps with existing legislation" (Artur Bogucki et al, "The AI Act and Emerging EU Digital Acquis: Overlaps, gaps and inconsistencies" (September 2022) at 1, online (pdf): *CEPS* <www.ceps.eu/download/publication/?id=37468&pdf=CEPS-In-depth-analysis-2022-02_The-AI-Act-and-emerging-EU-digital-acquis.pdf> [perma.cc/YA7F-JB8M]).

[114]   Bogucki et al, *supra* note 113, signal this as an issue in the EU.

[115]   This was enabled through statutory amendments contained in an Omnibus bill. The Advanced Therapeutic Pathway is still under development (Strategies and Initiatives, "Regulatory innovation for health products: Enabling advanced therapeutic products" (last modified 28 January 2022), online: *Government of Canada* <www.canada.ca/en/health-canada/corporate/about-health-canada/activities-responsibilities/strategies-initiatives/health-products-food-regulatory-modernization/advanced-therapeutic-products.html> [perma.cc/QFP6-YB7F]). For a discussion of the reform of the legislation to enable this new approach, see Vural, Herder & Graham, *supra* note 62.

[116]   CSA Regulatory Sandbox, *supra* note 55.

been considering how to build safety and security into its regulation of automated vehicles.[117] The Treasury Board Secretariat has developed a risk regulation framework for ADS adopted by government.[118] Because the *AIDA* is an overarching statutory framework, the desire not to excessively overlap or interfere with these other governance efforts has undoubtedly shaped its structure, although the absence of a definition of 'high impact' AI makes it hard to fully assess its scope.

In addition to potential overlaps with other departments or agencies in their regulation of AI-enabled technologies, there are also substantive areas of potential overlap between the *AIDA* and other regimes. For example, the *AIDA* proposes to address the problem of 'biased output' in AI technologies. That this overlaps with the Canadian Human Rights Commission's jurisdiction over human rights is underscored by the adoption, in the definition of "biased output"[119] of the prohibited grounds of discrimination from the *Canadian Human Rights Act*.[120] An AI system that adversely impacts an individual on the basis of a prohibited ground of discrimination under the *CHRA* with respect to subject matter covered by that statute[121] could provide the basis for a complaint under the *CHRA*. The same system would be subject to governance under the *AIDA* if it also met the elusive definition of 'high impact'. The role of the *AIDA* is framed as providing *ex ante* regulation, while the *CHRA* will provide an *ex post* complaints mechanism. However, with its experience in human rights, an alternative could have been to give the Canadian Human Rights Commission a clearer and more proactive role in the regulation of discriminatory bias in AI.

Another area of overlap is found in the governance of human-derived data. Personal data protection is the domain of the Privacy Commissioner of Canada, both for the public sector and the private sector where *PIPEDA* applies. The core obligations with respect to data under the *AIDA* are found in clause 6, and apply to a person who carries out a regulated activity *and* who "processes or makes available for use anonymized data in the course of that activity."[122] The definition of "regulated activity" includes processing or making available for use "any data relating to human activities for the

---

[117]   Transport Canada, "Canada's Safety Framework for Automated and Connected Vehicles" (February 2019), online (pdf): <tc.canada.ca/sites/default/files/2020-05/tc_safety_framework_for_acv-s.pdf> [perma.cc/VU63-V4UM].

[118]   DADM, *supra* note 89.

[119]   *AIDA*, *supra* note 1, cl 5(1).

[120]   RSC 1985, c H-6 [*CHRA*].

[121]   This includes the provision of goods, services or facilities, commercial premises or residential accommodation, or in employment or hiring *(ibid*, ss 5–11).

[122]   *AIDA*, *supra* note 1, cl 6.

purpose of designing, developing or using" an AI system.[123] To address any potential overlap, the *CPPA* will specifically exclude anonymized data from its scope in clause 6(5), which provides that: "[f]or greater certainty, this Act does not apply in respect of personal information that has been anonymized."[124] In Bill C-27, the choice is clearly to separate anonymized data from personal data, leaving only the latter under the governance of the Privacy Commissioner. The result may lead to some confusion, as not all data used in AI are anonymized personal data, creating the potential both for governance overlap and gaps. For example, the definition of anonymized data in 'absolute' terms in the *CPPA* in the data protection part of Bill C-27, the lack of definition of anonymized data in the *AIDA*, and the fact that the *AIDA* will not apply to many actors, means that the nature and extent of governance of anonymized data is both uncertain and likely to be incomplete.

Canada is also in the process of developing online harm legislation, which may or may not address algorithms used in this context.[125] The Competition Bureau is examining its role in relation to how AI and algorithms may be used in anti-competitive practices.[126] It is unclear how any potential overlaps with the *AIDA* will be managed where there are overlaps with other regulatory schemes, although the answer may be in the eventual definition of a high-impact system and any exclusions added to the definition.

The potential for overlaps is acknowledged in the *AIDA*. Under clause 26(1), the Minister may disclose any information she or he obtains in administering the Act to specified entities if she or he has reasonable grounds to believe that a person carrying out a regulated activity "has contravened, or is likely to contravene, another Act of Parliament or a provincial legislature."[127] Those entities are the regulators likely to be responsible for such contraventions, and include the Privacy Commissioner, the Canadian Human Rights Commission, the Commissioner of Competition, the Canadian Radio-television and Telecommunications Commission, their provincial analogues, or any other person prescribed by regulation. These other laws have *ex post* complaint and investigation mechanisms, which

---

[123]   *Ibid*, cl 5(1).

[124]   *CPPA*, *supra* note 1, cl 6(5).

[125]   See Canadian Heritage, "Technical paper" (last modified 29 April 2022), online: *Government of Canada* <www.canada.ca/en/canadian-heritage/campaigns/harmful-online-content/technical-paper.html> [perma.cc/4XF2-F8G3].

[126]   Competition Bureau, "Big data and innovation: key themes for competition policy in Canada" (last modified 20 January 2022), online: *Government of Canada* <www.competitionbureau.gc.ca/eic/site/cb-bc.nsf/eng/04342.html> [perma.cc/E6SH-S5Q2].

[127]   *CPPA*, *supra* note 1, cl 26(1).

may or may not be compensatory, suggesting an *ex ante/ex post* split.[128] Nevertheless, many regulatory regimes with complaints mechanisms also have an *ex ante* dimension (e.g., data protection which is primarily focused on systemic change to improve data protection practices) which is primarily focused on systemic change to improve data protection practices.

B) Division of Powers

The second constraint relates to the legislative authority of the federal government within the constitutional framework of a federal state. Unlike a unitary state, in a federal state there are simply some areas where the national government lacks jurisdiction, or where the powers of the federal and state/provincial governments overlap. This reality will shape its legislative and regulatory activities.[129] The division of powers has proven particularly challenging in the context of digital technologies in Canada.[130] *PIPEDA*, Canada's first national private sector data protection law applied only to the collection, use, and disclosure of personal information in the course of "commercial activity," because the constitutionality of the law had to be premised on the federal general trade and commerce power.[131] Even so, the law faced early constitutional challenges.[132] The recent split decision of the Supreme Court of Canada regarding the constitutionality of

---

[128]   For example, compensation is available in proceedings under the *CHRA*, *supra* note 120, s 53(2). It is also possible to seek compensation for breaches of *PIPEDA*, *supra* note 4, s 16(c). Recourse may also be available in tort law or under *Civil Code of Québec*, CCQ. See Thomasen, *supra* note 81.

[129]   For a discussion of the impacts of federalism on the regulation of AI in the US, see Céline Castets-Renard, "AI and the Law in the European Union and the United States" in Florian Martin-Bariteau & Teresa Scassa, eds, *Artificial Intelligence and the Law in Canada* (Toronto: LexisNexis Canada, 2021) 377 at 397–401.

[130]   Most recently, consider the constitutional challenge to *CASL*, *supra* note 67, in *3510395 Canada Inc v Canada (AG)*, 2020 FCA 103. In that case, the Federal Court of Appeal ruled that the anti-spam legislation was a valid exercise of the federal general trade and commerce power.

[131]   Barbara Von Tigerstrom, *Information & Privacy Law in Canada*, (Toronto: Irwin Law, 2020) at 293; Frank Addario & Samara Secter, "The Constitutional Validity of Bill C-11, the *Digital Charter Implementation Act*" (31 March 2022), online: *Office of the Privacy Commissioner of Canada* <www.priv.gc.ca/en/opc-news/news-and-announcements /2022/op-c11_addario/> [perma.cc/5D3B-A848].

[132]   On December 17, 2003, the Quebec government indicated its intention to pursue a reference case before the Quebec Court of Appeal regarding the constitutionality of *PIPEDA* (Gouvernement du Québec, Decret No 1368–2003 (14 January 2004) 136:2 Q Gaz II, 184, online (pdf): <www.publicationsduquebec.gouv.qc.ca/fileadmin/gazette/ pdf_encrypte/lois_reglements/2004F/41778.pdf> [perma.cc/]). The challenge was abandoned. Constitutionality issues were also raised, but not resolved, in *State Farm Mutual Automobile Insurance Company v Privacy Commissioner of Canada*, 2010 FC 736.

the *Genetic Non-Discrimination Act*[133] also demonstrates the difficulty of locating constitutional authority in the face of technological developments that create new risks.[134]

The government's desire to stay on the right side of its constitutional authority is evident in Bill C-27, with the *CPPA* not only retaining the limit on scope of application to "commercial activit[y],"[135] but reinforcing this limitation in its new name: the *Consumer Privacy Protection Act* [added emphasis]. Similar jurisdictional preoccupations are evident in the *AIDA*. Clause 4 sets out the dual purposes of the statute, which are expressly rooted in the federal government's authority:

> a) to regulate international and interprovincial trade and commerce in artificial intelligence 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 artificial intelligence systems that may result in serious harm to individuals or harm to their interests.[136]

By focusing on international and interprovincial trade and commerce, the government asserts its general trade and commerce jurisdiction, without treading on the toes of the provinces, which remain responsible for intra-provincial activities. The prohibition of conduct that may result in serious harm also appears to invoke the federal criminal law power, although it ultimately does so in a circular way that limits it only to international and interprovincial trade and commerce.[137]

It is important to note that, in spite of superficial similarities, the *AIDA* does not replicate the *PIPEDA*'s (and the *CPPA*'s) scheme wherein the legislation applies by default to those involved in intra-provincial commercial activity unless a province has enacted substantially similar

---

133   SC 2017, c 3.
134   *Reference re Genetic NonDiscrimination Act*, 2020 SCC 17.
135   *CPPA*, *supra* note 1, cl 6.
136   *AIDA*, *supra* note 1, cl 4.
137   Clause 4(b) of the *AIDA, ibid*, suggests that at least when it comes to AI systems that may result in serious harm, the federal jurisdiction over criminal law may be invoked. The *AIDA* creates a series of offences that could be supported by this power. However, these offences relate to failures to meet the obligations that arise from engaging in a 'regulated activity'—which must be carried out in the course of international or interprovincial trade and commerce. The federal trade and commerce power thus remains the backbone of this bill.

legislation.[138] The *PIPEDA* operates in a context where what is important is the commercial nature of an *activity* in which data flows from an individual to an organization. If that exchange of data is in the course of commercial activity, the *PIPEDA* applies. The *AIDA* is different. Because of its *ex ante* regulatory approach, it applies to a range of different activities that include "designing, developing or making available for use an artificial intelligence system or managing its operations."[139] Many of the activities are internal to a company's operations and do not depend on a particular transaction or whether it is commercial in nature. If the goal is to regulate high-impact AI systems at the design and development stage, the focus cannot be on the commercial or non-commercial nature of a transaction that takes place at the end of the process. Instead, under the *AIDA*, whether these activities are in the course of "international or interprovincial trade and commerce" ultimately depends upon the nature of the organization and its activities.[140] Thus, to determine whether the law applies, the questions to ask are whether the organization is a for-profit entity and whether it has customers in Canada who are outside of the province or country where it is headquartered. If the answer to these questions is yes, presumably the organization is subject to the *AIDA* with respect to its AI activities in Canada. Interestingly, it may well be that some companies subject to the *AIDA*'s rules on the governance of anonymized data will also need to comply with provincial rules regarding anonymization. For example, a company in Quebec that produces 'high impact' AI systems would have to comply with Quebec's new law which will set standards for anonymization,[141] but would also have to comply with the *AIDA*'s rules for anonymization if its products, services or activities crossed provincial boundaries. For offshore companies, compliance with the *AIDA* would be required where high-impact products, services or activities reached Canadian customers—even though this might happen long after the design or development stage.

By focusing—for general application purposes—on the status of the supplier rather than the customer, governance under the *AIDA* may oddly be more inclusive than the *PIPEDA* has been in the past. For example, the law would presumably apply to off-the shelf or custom-built AI systems used by those provincial and federal government departments or agencies that are not specifically excluded by clause 3(2) of the *AIDA*, as well as

---

138   See *PIPEDA*, *supra* note 4, s 26(2); *CPPA*, *supra* note 1, cl 122(2) and (3). Three provinces (Quebec, Alberta and British Columbia) enacted private sector data protection laws that were considered 'substantially similar' under *PIPEDA*.

139   *AIDA*, *supra* note 1, cl 5(1), definition "regulated activity".

140   *Ibid*, cl 4(a).

141   See *An Act to modernize legislative provisions as regards the protection of personal information*, SQ 2021, c 25, s 28.

by non-profits and by political parties, although the bulk of the *AIDA*'s statutory obligations fall on the supplier rather than the customer for the system. Yet where the exemption in clause 3(2) applies, we see a further structural constraint—the separation of public and private sectors.

C) Public and Private Sectors

The third structural constraint is the distinction between public and private sectors. Although this is not the most significant of the constraints, it can create challenges. Public sector actors face different circumstances or priorities than those in the private sector; this can justify separate legislative approaches. However, it is not always the case that bright lines need to be drawn between the two. For example, rather than create two separate data protection regimes for public and private sector actors, the EU's *General Data Protection Regulation* applies to those in both public and private sectors, although some modifications are available in the case of public sector actors.[142] The EU AI Act follows a similar model to the *GDPR*. By contrast, Canada has traditionally followed a model of data protection that firmly separates public from private sector governance at both federal and provincial levels. To make matters more complicated, at the federal level, governance of personal data in the public sector has been under the authority of the Minister of Justice, whereas private sector data protection law comes from the Minister of Innovation, Science and Industry.[143] Although both the private and public sector data protection laws have been long overdue for reform, the reform has not proceeded on the same timetable, or via the same policy makers. By contrast, although the provinces have tended to replicate the public/private sector divide when it comes to governance of personal data, the province of Quebec's 2021 privacy reform legislation addressed both its public and private sector laws, as well as consequential amendments required to any other provincial laws.[144] In doing so, it both acknowledged that different considerations may affect the rules for public and private sector actors when it comes to personal data, but that at the same time the two schemes should be rationally co-ordinated, sharing definitions and approaches.

AI governance in Canada seems destined to follow the same public/private sector split, with AI risk management for the federal public sector

---

[142]   EU, *General Data Protection Regulation*, 2016/679 [*GDPR*].

[143]   Admittedly, the division of powers issues discussed in Part 3 above also impact how the federal government proceeds, making it more challenging for it to fully co-ordinate its data protection laws across both public and private sectors.

[144]   This bill was passed into law in September 2021. See Bill 64, *An Act to modernize legislative provisions as regards the protection of personal information*, 1st Sess, 42nd Leg, Quebec, 2021 (assented to 22 September 2021) SQ 2021, c 25.

falling under the DADM. The DADM is developed and overseen by the Treasury Board Secretariat, while the *AIDA* will be the responsibility of the Minister. The *AIDA* expressly provides that it does not apply to any federal government institution as set out in the *Privacy Act*.[145] Presumably this means that while obligations under the *AIDA* may fall on the *supplier* of an AI system to government at the design and development stage, none will fall on the government institution that acquires the technology. It will also mean that AI systems developed in-house by government would not be subject to the *AIDA*. A similar circumstance likely *de facto* exists with respect to provincial governments, as the federal law cannot constitutionally regulate those governments or their in-house activities. Further, the *AIDA* does not apply to any product, service or activity that is under the direction or control of the Minister of National Defence, the Director of the Canadian Security Intelligence Service, or the Chief of the Communications Security Establishment.[146] These blanket exclusions are significant, since they would also preclude AI governance for systems used by these actors for recruitment, employee management, or other non-security-critical purposes.[147] As noted above, the *AIDA* will also not apply to "any other person who is responsible for a federal or provincial department or agency and who is prescribed by regulation."[148] The list of exclusions will no doubt continue to grow.

The result will be important gaps in AI governance that may or may not be filled by other frameworks. Action by each of Canada's provinces and territories will therefore need to put in place governance frameworks

---

[145]   *AIDA*, *supra* note 1, cl 3(1), referencing s 3 of the *Privacy Act*, RSC 1985, c P-21.

[146]   *Ibid*, cl 3(2).

[147]   In contrast, the EU's AI Act, *supra* note 76, art 2(3) addresses the perceived need for latitude when it comes to national defence via an exception for "AI systems developed or used *exclusively for military purposes*" [added emphasis]. This exception is nowhere near as broad as that in the *AIDA*, *ibid*, cl 3(2)(a) which excludes all products, services or activities under the control of the Minister of National defence. Note that the Department of National Defence (DND) made headlines in 2020 when it contracted for an AI application to assist in hiring (Tom Cardoso & Bill Curry, "National Defence skirted federal rules in using artificial intelligence, privacy commissioner says" (last updated 8 February 2021), online: *Globe and Mail* <www.theglobeandmail.com/canada/article-national -defence-skirted-federal-rules-in-using-artificial/> [perma.cc/BR9W-TRRM]); it also made headlines in 2021 over an aborted psyops campaign in Canada (Murray Brewster & Ashley Burke, "Military campaign to influence public opinion continued after defence chief shut it down" (24 June 2021), online: *CBC* <www.cbc.ca/news/politics/psychological-warfare-influence-campaign-canadian-armed-forces-1.6079084> [perma.cc/4R2H-SRGT]. It is unclear why non-military DND uses of AI should not be subject to governance.

[148]   *AIDA*, *supra* note 1, cl 3(2)(d).

for public sector AI as well as for AI-related activity that is entirely intra-provincial.[149]

4. Conclusion

In this paper I have set out some of the structural constraints that have shaped the *AIDA*. I have also considered its nature as risk regulation as well as the government's aspiration for it to be agile. I argue that it bears little resemblance to agile regulation, conflating extensive deferred regulation-making with agility. And, although it has many features of risk regulation, it is most notably missing an actual regulator.

It may be that substantial structural constraints go some way to explaining the difficulties with the *AIDA* and its failure to be both agile and a strong example of risk regulation. Canada's federal system means that the federal government lacks the constitutional authority to shape AI regulation in the same way as governments of unitary states. It also lacks the strong centralizing frameworks of the EU. Even without this, however, there may be missed opportunities for the federal government to be a national consensus-builder around the development of strong governance frameworks. Although the US is often characterized as taking 'light touch' approaches that signal a particular ideological approach to the regulation of technology,[150] the US approach may also be conditioned by its federal state structure, proposing a detailed voluntary and consensus framework, rather than a national regulator. Certainly, in the US the states remain free to act and many have begun to do so.[151]

What should the Canadian government be doing to regulate AI in this context? Building federal-provincial cooperation and collaboration on norms and standards to guide industry is one important area of activity. Convening stakeholders and building frameworks is another. In this respect the lack of consultation in the *AIDA* is a matter of particular concern. Consensus-building and norm-setting can support the work of existing regulators and agencies, and can buttress *ex post* remedial processes by establishing standards and norms for AI applications. The government should also consider providing more funding and new power to existing regulators in their *ex ante* and *ex post* roles—especially

---

[149]   Work is moving forward to develop such frameworks in some provinces. For example, Ontario has been consulting on the development of a Responsible AI Framework (Government Data, "Consultation: Ontario's Trustworthy Artificial Intelligence (AI) Framework" (last updated 9 March 2023), online: *Government of Ontario* <www.ontario.ca/page/ontarios-trustworthy-artificial-intelligence-ai-framework-consultations> [perma.cc/6YCU-YJQ4]).

[150]   Castets-Renard, *supra* note 129 at 404.

[151]   *Ibid* at 411–15.

to those with cross-sectoral authority such as the Commissioners of Competition, Privacy, and Human Rights. They should also consider providing additional authority, as necessary, to regulators in sectors strongly impacted by AI innovation, including Transportation, Health, and Finance. These regulators could enhance their supervisory authority and their capacity to monitor and deal with high-risk AI in their sectors; they could also provide the regulatory bodies with additional flexibility to enable experimentation with agile forms of regulation such as regulatory sandboxes. The government should also consider the creation of an independent agency—or the empowering of an existing agency— to oversee the kind of regulatory scheme contemplated in the *AIDA*. Challenging the *AIDA* does not mean that there cannot and should not be AI regulation in Canada; but such regulation, when it comes, must be the product of much greater consultation and collaboration, and must be rationally integrated with existing and emerging frameworks.