Beyond Bill C-27: From AI Legislative Gaps to a Reformed AI and Data Act

Mirwaaj Afzal
Queen's University
23fpj@queensu.ca

Sylvia Shi
Queen's University
20bs31@queensu.ca

Shahnoor Sarfraz
Queen's University
23tn40@queensu.ca

Neethan Jayaseelan
Queen's University
neethan.jayaseelan@queensu.ca

Kate Sigurdson
Queen's University
23sxn2@queensu.ca

***Abstract*—Artificial intelligence systems are increasingly used in areas that affect people's daily lives, yet Canada does not have a clear and enforceable federal law governing their use. Bill C-27, through the proposed Artificial Intelligence and Data Act (AIDA), attempted to address this gap but relied too heavily on future regulations and broad definitions.**

This paper examines the weaknesses of AIDA through legislative analysis, case studies, and comparison with international models. It proposes targeted amendments to clarify definitions, strengthen accountability, and improve enforcement, with the goal of creating a clearer and more effective framework for regulating high-impact AI systems in Canada.

I. Introduction/Precis

A. Background

Artificial intelligence (AI) systems are increasingly deployed in domains that affect employment, healthcare, finance, education, public discourse, and access to essential services. Despite their growing influence, AI systems in Canada remain largely unregulated at the federal level. In practice, their design, deployment, and governance are controlled predominantly by private-sector actors, whose terms of service and end-user license agreements (EULAs) structure accountability and allocate risk in their favor. This creates a governance asymmetry in which individuals are subject to automated decision-making systems without corresponding statutory protections.

Existing Canadian privacy and human rights frameworks were not designed to regulate adaptive, large-scale AI systems, because they do not impose comprehensive obligations specific to algorithmic risk assessment, transparency, independent auditing, proportionality, or ongoing monitoring. The proposed Artificial Intelligence and Data Act attempted to address this gap; however, its reliance on future regulations, broad discretionary terminology, and high liability thresholds limit its capacity to function as a robust and preventative regime.

As a result, Canada faces a regulatory vacuum in which high-impact AI systems operate with limited statutory oversight, fragmented accountability, and insufficient enforcement clarity. This project examines the structural weaknesses of AIDA and proposes targeted legislative amendments to transform it from a largely discretionary framework into a clear, enforceable, and proportionate governance mechanism for artificial intelligence in Canada. [1]

B. The Failure of Bill C-27

In June 2022, the Minister of Innovation, Science and Industry, François-Philippe Champagne, introduced Bill C-27 before Parliament. [2] The bill was structured in three distinct parts. First, it proposed repealing and replacing the Personal Information Protection and Electronic Documents Act (PIPEDA) with the Consumer Privacy Protection Act (CPPA), modernizing Canada's private-sector privacy regime. Second, it sought to establish a Personal Information and Data Protection Tribunal to review certain decisions of the Privacy Commissioner, and thus, restructuring the enforcement architecture of federal privacy oversight. Third, and most significantly, it introduced the Artificial Intelligence and Data Act, Canada's first federal statute directed specifically at artificial intelligence systems.

While Bill C-27 represented an acknowledgment that Canada's existing legislative framework was inadequate for the dynamic technology industry, its design reflected limited structural change rather than comprehensive adaptation. Privacy reform under the CPPA continued to rely on models developed in earlier technological eras, and AIDA was embedded within a broader data governance bill rather than introduced as a standalone regulatory regime. This bundling of legislation diluted scrutiny on AI governance and framed artificial intelligence primarily as an extension of privacy regulation rather than as an autonomous area of risk on its own. Rather than constructing a fully independent AI regulatory model, the bill extended existing digital governance logic into several different contexts without fully addressing the distinct scale and autonomy of modern AI systems.

Ultimately, Bill C-27 did not complete the legislative process. The prorogation of the 44th Parliament resulted in the bill dying on the order paper, preventing final passage and Senate review. This procedural outcome, following extended committee consideration and debate, left Canada without enacted federal AI legislation.

1) Reform of PIPEDA to CPPA: The reform of the Personal Information Protection and Electronic Documents Act (PIPEDA) into the Consumer Privacy Protection Act (CPPA) was framed as a modernization of Canada's private-sector privacy regime. The CPPA aimed to strengthen consent requirements, enhance individual control over personal information, introduce increased penalties for non-compliance, and

establish clearer obligations regarding data transparency. It also proposed the creation of a Personal Information and Data Protection Tribunal to review certain decisions of the Privacy Commissioner, reshaping the architecture of federal privacy oversight.

Despite these structural revisions, the reform remained rooted in a data protection paradigm rather than an artificial intelligence governance model. The CPPA continued to portray harm primarily in relation to information misuse, unauthorized disclosure, and inadequate consent. While these concerns are central to digital privacy, they do not sufficiently capture the operational dynamics of modern AI systems, which generate automated outputs and influence substantive decisions affecting individuals and groups. As such, the CPPA's framework did not fully address the systemic risks associated with AI system use.

2) Emergence of AIDA: The Artificial Intelligence and Data Act (AIDA) emerged as Canada's first attempt to regulate AI systems at the federal level. Positioned as Part 3 of Bill C-27, AIDA was intended to establish obligations for persons responsible for high-impact AI systems. It also introduced administrative monetary penalties and criminal offences for certain forms of non-compliance or reckless deployment which result in serious harm.

However, rather than expressing a comprehensive statutory framework, AIDA relied heavily on regulatory discretion. Core concepts, including the criteria for classifying a system as "high-impact," were deferred to future regulations. This regulatory delay meant that Parliament enacted a skeletal framework without clearly defining the scope of its most consequential provisions.

3) Failure of AIDA: AIDA left an extremely broad lens on definitions, including criteria for defining "high-impact systems" and compliance requirements. Much of the substantive detail, including classification thresholds and enforcement mechanics, was deferred to future regulations. Parliament therefore advanced a framework that articulated general objectives while postponing essential decisions to executive rule-making. This legislative structure contributed to uncertainty, limited clarity about scope and enforcement, and ultimately weakened the ability of the bill to respond proportionately to the scale and complexity of AI deployment in Canada.

During its passage through the House of Commons, Bill C-27 and AIDA drew notable debate from multiple parties. Members of the political spectrum expressed concerns about the clarity of the definition, the technological neutrality, and the overall scope of AI regulation. Legislators emphasized the need for consistent, future-proof definitions of artificial intelligence and algorithmic systems to ensure the statute could adapt to evolving technologies. Some members further suggested that the breadth of the bill required clearer statutory constructs to effectively protect individuals and to maintain coherence with provincial privacy regimes. These parliamentary critiques reflected broader uncertainty about whether the statutory framework, as drafted, provided sufficient precision to function as a durable governance model.

Beyond parliamentary debate, current commentary highlighted concerns regarding insufficient public consultation and stakeholder engagement during the drafting and review process. Civil society groups, industry stakeholders, and labour advocates argued that the legislative process did not adequately incorporate diverse perspectives, particularly with respect to workers' rights, public interest safeguards, and the societal implications of automated decision-making systems. The limited depth of structured public engagement narrowed the deliberative legitimacy of Canada's first federal attempt at AI regulation.

The failure of AIDA was therefore not only substantive but procedural. Structural ambiguities, limited public consultation, and parliamentary interruption collectively contributed to its collapse, leaving artificial intelligence largely within the regulatory discretion of private actors rather than under a comprehensive federal statutory regime.

C. Importance of AI Regulation

The regulatory shortcomings identified above are not merely theoretical. Artificial intelligence systems are already deployed in contexts that materially affect access to employment, housing, credit, education, healthcare, public services, and public discourse. When such systems operate without clear statutory obligations relating to risk classification, transparency, independent auditing, and proportionality, accountability becomes fragmented and reactive. Individuals bear the consequences of automated decisions while relying on outdated legal instruments not designed for adaptive, inference-based systems operating at scale.

The absence of a coherent AI governance regime also creates institutional uncertainty. Regulators must interpret traditional privacy and human rights statutes in novel technological contexts, while organizations operate within ambiguous compliance expectations. This environment undermines legal predictability and weakens public trust. As AI deployment accelerates across sectors, the failure to establish a clear, enforceable, and proportionate federal framework risks entrenching governance asymmetries in which technological power outpaces legislative control.

D. Thesis

This paper analyzes why Bill C-27, particularly AIDA, fails to adequately regulate the evolving dynamics of artificial intelligence and argues that existing Canadian legislation does not sufficiently account for the speed, scale, and risk profile of modern AI systems. By placing AIDA in comparative analysis with other AI regulatory models, this paper proposes legislative reforms to address these deficiencies.

E. Purpose of the Amendments

The purpose of these amendments is to transform AIDA from a largely discretionary and regulation-deferred framework into a structured, enforceable, and proportionate governance regime capable of responding to the evolving dynamics of artificial intelligence. The proposed reforms clarify definitions, expand

upon obligations, strengthen risk classification mechanisms, and close accountability gaps related to outsourcing, third-party components, and post-deployment surveillance.

Rather than relying on broad ministerial discretion and undefined regulatory thresholds, the amendments embed core compliance standards directly within the statute. This approach enhances legal certainty, ensures consistent application of enforcement powers, and aligns oversight mechanisms with the technical realities of adaptive AI systems. In doing so, the amendments seek to put preventative governance into effect rather than regulation.

F. Conclusion

Canada's attempt to regulate artificial intelligence through Bill C-27 marked an important acknowledgment of emerging technological risk, yet it ultimately fell short of establishing a clear and enforceable governance regime. By embedding AIDA within a broader privacy reform bill, deferring critical definitions to future regulations, and leaving substantial discretion to the executive, Parliament advanced a framework that lacked structural precision and preventative force.

This paper contends that effective AI governance requires statutory clarity, lifecycle-based accountability, and enforceable obligations proportionate to system risk. The following sections examine the deficiencies of the current framework and advance amendments designed to transform AIDA into a coherent, risk-responsive, and durable legislative instrument capable of regulating artificial intelligence in Canada.

II. Legal Context and Comparative Analysis

A. Case Studies: The Necessity of AI Legislation

The following cases demonstrate that artificial intelligence is no longer hypothetical in Canada. These systems are already being tested, deployed, and integrated into public and commercial infrastructure. However, the legal responses remain reactive and fragmented, revealing structural weaknesses in the existing framework and limitations within the original AIDA model.

1) Canada Border Services Agency Facial Recognition Proposal: The Canada Border Services Agency has explored implementing smartphone-based facial recognition technology to verify traveler identity at border crossings. [3] Although the system has not been fully deployed, the proposal immediately raised concerns regarding biometric surveillance, algorithmic error, and the normalization of facial recognition in public governance.

Under current Canadian law, oversight would primarily arise through the Privacy Act or potentially Sections 7 and 8 of the Charter. Both instruments operate reactively, either through complaints or constitutional litigation after harm or rights infringement has occurred. Neither statute imposes mandatory impact assessments before biometric systems are introduced, nor do they require ongoing algorithmic monitoring.

Under AIDA as originally drafted, the applicability of the Act would depend on whether the initiative fell within "regulated activity" in the course of trade and commerce. Because AIDA was structured primarily around commercial actors, its application to federal agencies engaging in biometric verification was not clearly articulated. Further, whether such a system would qualify as "high-impact" depended entirely on future regulations. The statute itself did not provide fixed classification thresholds. As a result, even a large-scale biometric identification system affecting mobility and identity verification would operate within a framework of regulatory discretion rather than statutory precision.

2) Mental Health Chatbots and Psychological Risk: AI-driven mental health chatbots marketed as therapeutic tools have raised concerns about psychological harm, user over-reliance, and the commercial exploitation of sensitive conversational data. [4] Users disclose highly personal information to systems that generate automated responses without licensed clinical oversight.

Current regulation occurs primarily through PIPEDA, which addresses commercial data collection and disclosure. However, PIPEDA focuses on consent and data misuse, not on the substantive safety of automated advice. The law does not meaningfully regulate the psychological impact of algorithmic outputs or establish clear liability for harmful guidance generated by AI systems.

Under AIDA's initial framework, such systems would only trigger enhanced obligations if classified as 'high-impact,' a determination left to regulation rather than statute. The Act did not define psychological vulnerability, cumulative harm, or significant automated decision-making with precision. Without explicit thresholds, consumer-facing AI systems influencing mental health would exist within uncertainty, dependent on executive regulation rather than nested legislative standards.

3) University of Waterloo Facial Recognition Vending Machines: In 2024, students at the University of Waterloo discovered that campus vending machines incorporated AI-powered facial recognition technology without meaningful notice or consent. [5] The collection of biometric data prompted privacy complaints and regulatory review under Ontario's Freedom of Information and Protection of Privacy Act.

The legal response addressed the matter as an informational privacy breach. While the provincial statute provided remedial oversight, the issue was treated as improper data collection rather than as a broader AI governance concern involving biometric surveillance and automated inference systems.

Under the original AIDA structure, applicability again depended on whether the activity constituted regulated trade and commerce. Universities, as public institutions, do not clearly fall within the commercial orientation of the statute. Moreover, the classification of such biometric systems as "high-impact" would have required regulatory definition. The statute itself did not clearly impose reassessment obligations or specify how third-party AI components integrated into institutional infrastructure should be governed.

These cases reveal a consistent pattern; Canadian law addresses AI harms primarily through privacy statutes after issues emerge, rather than through structured, preventative

AI governance. The original AIDA framework acknowledged the need for federal intervention, but its reliance on undefined regulatory criteria and classification left up to federal discretion limited its capacity to provide clear, immediate oversight of emerging AI sxystems.

B. Comparative Analysis

AIDA was drafted as Canada's first federal attempt to regulate artificial intelligence, but its statutory design diverged significantly from major peer approaches. A comparative analysis against the European Union Artificial Intelligence Act (EU AI Act) and the United States' 2023 Executive Order on Safe, Secure, and Trustworthy Artificial Intelligence illustrates that AIDA was comparatively under-specified at the statutory level, relied heavily on future regulations to define its core scope, and offered less immediate clarity regarding coverage, duties, and enforcement triggers.

1) EU AI Act: Statute-Level Risk Architecture: The EU AI Act is built around an explicit, statute-level risk architecture. [6] It distinguishes prohibited practices, high-risk systems, and targeted transparency duties, and it allocates responsibilities across the AI supply chain. In practical terms, the Act is designed to operate as an ex ante compliance regime. Core obligations attach before and during deployment, rather than only after harm occurs. High-risk systems are governed through structured requirements such as documentation, risk management, data governance expectations, human oversight, and conformity assessment logic.

This approach matters because it reduces dependence on executive discretion for threshold-setting. The primary categories that determine whether obligations apply are anchored in the legislative text, which increases predictability for regulated actors and reduces ambiguity for regulators. The EU model treats AI governance as a distinct regulatory domain rather than as a subset of privacy law. It therefore frames risk not only in terms of informational misuse, but also in terms of systemic impact, safety, and rights-based harms that arise from automated decision-making.

By comparison, AIDA did not embed a similarly detailed statute-level risk taxonomy. Its key gatekeeping concept, the 'high-impact system,' was defined by reference to criteria established in future regulations, leaving scope and coverage contingent on later executive rule-making.

2) United States: Executive Order as Coordinated Federal Governance: The United States has not enacted a single comprehensive federal AI statute analogous to the EU AI Act. [7] Instead, the most prominent national-level instrument is the 2023 Executive Order on Safe, Secure, and Trustworthy Artificial Intelligence. The Executive Order functions as an executive-driven governance mechanism that coordinates agency action, directs the development of technical standards, and sets expectations for safety evaluation of advanced models.

As a governance approach, the Executive Order is operationally immediate. It can direct federal departments to develop guidance, procurement standards, and technical evaluation procedures without waiting for a full legislative cycle. It also emphasizes the role of technical standards and risk management practices, positioning safety testing and evaluation as central levers of federal oversight. However, because the Executive Order is an executive instrument rather than a statute, it does not create a unified legislative enforcement framework with codified penalties, independent statutory oversight architecture, or stable statutory rights of redress. Its durability and scope are tied to executive authority and agency implementation.

Relative to AIDA, this U.S. approach provides faster administrative direction and standard-setting, but less statutory certainty as law. Conversely, AIDA aimed to establish a formal legislative structure with administrative and criminal penalties, but deferred the most critical scope-defining elements to future regulations. The result is a trade-off: the U.S. framework is more immediately operational through executive coordination, while AIDA, as drafted, offered a legislative skeleton awaiting regulatory substance.

3) AIDA: Regulation-Deferred Scope and Discretion-Heavy Enforcement Triggers: AIDA attempted to regulate AI through a framework focused on high-impact systems, compliance duties, and ministerial enforcement powers. However, the Act's core scope hinged on regulation-deferred classification. The statute did not define the criteria for "high-impact" within the Act itself, and many of its practical enforcement triggers depended on future regulatory decisions. This structure reduced immediate clarity regarding which systems would be captured, how duties would apply across different deployment contexts, and how enforcement would scale with severity of harm. [8].

In addition, AIDA was embedded within a broader data governance bill rather than introduced as a standalone AI statute. This legislative bundling framed AI governance as adjacent to privacy reform rather than as a discrete area of risk requiring its own regulatory philosophy. In effect, AIDA acknowledged that AI required oversight, but it preserved a discretionary and under-specified architecture at precisely the points where statutory precision determines enforceability. This helps explain why AIDA was widely criticized as vague, difficult to implement, and structurally dependent on later rule-making for legitimacy and function.

4) Comparative Synthesis: In comparative terms, the EU AI Act embeds a statute-level risk taxonomy and ex ante compliance obligations that attach through clear legislative categories. The United States relies on executive coordination through the 2023 Executive Order, emphasizing technical standards, safety evaluation, and agency-led implementation rather than a single binding federal AI statute. AIDA, as drafted, attempted to create a Canadian statutory regime, but it deferred its core coverage thresholds and key operational details to future regulations, leaving the Act less determinate than the EU model and less immediately operational than the U.S. executive-driven approach.

AIDA's legislative structure prioritized flexibility and discretion where statutory clarity is most necessary for consistent compliance expectations, effective enforcement, and public legitimacy in the face of rapidly scaling AI deployment.

C. Stakeholder and Institutional Perspectives

The debate surrounding AIDA was not limited to Parliament. Civil society organizations, academic researchers, labour groups, and industry stakeholders all raised concerns regarding the structure and clarity of the proposed framework. While many supported the recognition that AI requires federal oversight, critiques focused on definitional ambiguity, concentration of discretion in the executive, and insufficient statutory safeguards.

Privacy advocates emphasized that deferring key classifications to future regulation risked weakening accountability. Without fixed statutory thresholds for high-impact systems, enforcement would depend heavily on ministerial interpretation. This created uncertainty regarding when obligations would apply and how consistently they would be enforced. Concerns were also raised regarding transparency, particularly with respect to audit processes and publication powers, and whether confidentiality claims could limit meaningful public oversight.

Labour organizations highlighted risks related to automated decision-making in employment contexts, including algorithmic hiring, productivity monitoring, and workplace surveillance. They argued that AI systems affecting livelihood and workplace rights required clearer protections and consultation mechanisms. At the same time, industry stakeholders expressed concern about regulatory unpredictability, noting that broad and undefined obligations could create compliance uncertainty without clear guidance.

Institutionally, regulators faced a structural challenge. The Office of the Privacy Commissioner was positioned within a privacy framework, while AIDA proposed a separate enforcement structure led by ministerial authority. This created questions about institutional coordination and whether Canada's oversight bodies were equipped with the technical capacity required for effective AI supervision.

These stakeholder perspectives reinforce a central theme of this paper: that effective AI governance requires statutory clarity, institutional coordination, and structured accountability rather than broad, regulation-deferred discretion.

D. Summary of Identified Deficiencies in AIDA

The analysis above reveals several structural deficiencies within the original AIDA framework. First, the Act relied heavily on future regulations to define its most consequential concepts, including the classification of high-impact systems. This regulation-deferred approach reduced immediate clarity regarding scope and enforcement.

Second, AIDA's definitions were narrow in certain respects and broad in others. While the Act attempted to define artificial intelligence systems and harm, it did not clearly account for cumulative risk, systemic discrimination, or lifecycle modifications after deployment. As AI systems evolve over time through updates and integration with third-party components, these omissions create regulatory gaps.

Third, the enforcement model concentrated significant discretion within ministerial authority without embedding detailed compliance triggers directly into the statute. Although administrative penalties and criminal liability were included, the thresholds for activation depended on undefined or regulation-based standards. This weakened the preventative character of the regime.

Fourth, AIDA was structurally embedded within a broader privacy reform bill. This bundling framed AI governance as an extension of data protection rather than as an independent regulatory domain. As demonstrated through the case studies and comparative analysis, modern AI systems introduce risks that exceed informational privacy alone.

Together, these deficiencies illustrate why AIDA, as drafted, struggled to provide clear, enforceable, and proportionate oversight of artificial intelligence. The following section advances amendments designed to address these structural weaknesses and establish a more coherent federal AI governance framework.

E. Proposed Amendments to AIDA

Rather than rewriting the entire legislative framework, the proposed amendments target definitional precision, lifecycle accountability, and enforcement clarity.

First, the amendments replace technique-based definitions of artificial intelligence with an inference-based standard that captures systems operating with autonomy and adaptiveness, regardless of computational method. The definition of "high-impact system" is embedded directly within the statute rather than deferred to regulation, ensuring that systems affecting employment, housing, credit, healthcare, and essential services are captured without executive discretion.

Second, the amendments introduce statutory definitions of "risk," "serious harm," "incident," and "material modification." These additions shift the framework from reactive liability toward preventative governance by requiring reassessment, monitoring, and mitigation throughout a system's lifecycle rather than only at deployment.

Third, accountability provisions are strengthened by clarifying that responsibility cannot be avoided through outsourcing or reliance on third-party components. The definition of "person responsible" is expanded to include integration and post-deployment management. Confidential business information protections are refined to prevent overbroad claims from undermining audit and publication obligations.

Collectively, these amendments move AIDA from a regulation-deferred and discretion-heavy structure toward a clearer, risk-responsive, and enforceable statutory regime.

F. Practical and Legal Impact of the Amendments

III. Conclusion

Canada's attempt to regulate artificial intelligence through Bill C-27 reflected an important recognition that existing privacy and human rights frameworks are not designed to govern adaptive, inference-based systems operating at scale. However, the original AIDA model did not establish a sufficiently clear and enforceable regime. Its reliance on regulation-deferred thresholds, particularly in defining 'high-impact systems,'

and its concentration of discretion within executive rule-making limited both the preventative character of the Act and the predictability required for consistent compliance. The procedural failure of Bill C-27 further compounded this gap, leaving Canadian AI governance largely dependent on reactive privacy oversight and fragmented legal instruments.

The case studies examined in this paper illustrate that AI-related harms in Canada are already emerging across public administration, consumer-facing services, and institutional infrastructure. These scenarios raise issues that extend beyond consent and information misuse, including biometric surveillance, psychological risk, automated inference, and limited accountability for downstream deployment. The comparative analysis further demonstrates that peer jurisdictions have moved toward clearer risk architectures and more operational governance mechanisms, whether through statute-level risk taxonomies, as in the EU AI Act, or coordinated federal implementation through executive direction, as in the United States.

In response, this paper proposed targeted amendments to AIDA intended to shift the framework from discretionary and regulation-deferred oversight toward statutory clarity, life time accountability, and enforceable risk-based governance. By embedding core definitions and classification thresholds directly into the Act, expanding key concepts such as risk, incident, and material modification, and strengthening accountability for third-party integration and post-deployment change, the amendments aim to ensure that obligations attach to high-impact systems in a consistent and predictable manner. The proposed enforcement and institutional reforms similarly support a regime that can function as preventative governance rather than post hoc correction.

Ultimately, effective AI regulation in Canada requires more than symbolic legislative recognition. It requires a statutory structure capable of governing AI systems as they exist in practice: dynamic, scalable, and embedded within decisions that materially affect individuals and groups. A reformed AIDA, grounded in clear definitions, proper obligations, and credible enforcement, would provide Canada with a more coherent federal framework that protects the public interest while maintaining legal certainty as AI deployment continues to accelerate.

References

[1] "Artificial intelligence and data act (aida), part 3 of bill c-27," Parliament of Canada, 2022.

[2] "Bill c-27: Digital charter implementation act, 2022," House of Commons of Canada, 44th Parliament, 1st Session, 2022.

[3] "Canada border services agency facial recognition proposal," OECD AI Policy Observatory, AI Incidents Monitor, 2024.

[4] "Mental health chatbots: Therapeutic misconceptions and privacy concerns," OECD AI Policy Observatory, AI Incidents Monitor, 2024.

[5] "University of waterloo facial recognition vending machines," OECD AI Policy Observatory, AI Incidents Monitor, 2024.

[6] "Regulation (eu) 2024/1689 on artificial intelligence (artificial intelligence act)," European Parliament and Council of the European Union, 2024.

[7] Executive Office of the President, "Executive order 14110: Safe, secure, and trustworthy development and use of artificial intelligence," 2023.

[8] Canadian Labour Congress, "Labour concerns regarding bill c-27 and artificial intelligence regulation," 2023.

Appendix A
Amendments to Existing Definitions and New Definitions

1. Artificial Intelligence System

A. Amendment

Section 2 of the Act is amended by replacing the definition of "artificial intelligence system" with the following:

Trigger

If a machine-based system is designed to operate with varying levels of autonomy and, for explicit or implicit objectives, infers from the input it receives how to generate outputs such as predictions, content, recommendations, or decisions,

Duty / Prohibition

The system shall be considered an artificial intelligence system for the purposes of this Act, regardless of the specific computational technique used, and including systems that exhibit adaptiveness after deployment or materially influence physical or virtual environments.

Enforcement

The Minister or designated regulatory authority may determine whether a system falls within this definition when assessing compliance obligations, classification as high-impact, or the imposition of administrative or criminal penalties.

B. Rationale

The current AIDA definition is technique-based and identifies specific computational methods. The amended clauses involving negligence-based liability (s.39), algorithmic impact assessments, ongoing monitoring, and mandatory audits) expand regulatory scrutiny to system behavior and risk, not merely to the technology used. An inference-based definition ensures those obligations apply to any system that makes or influences decisions autonomously, regardless of how it is built. This prevents underinclusive enforcement and ensures that high-impact classification and penalty provisions operate as intended.

2. High-Impact System

A. Amendment

Section 5(1) of the Act is amended by replacing the definition of "high-impact system" with the following:

Trigger

If an artificial intelligence system is designed, developed, made available for use, or operated in a manner that materially affects access to employment, housing, credit, education, healthcare, essential services, law enforcement-related decisions, or otherwise creates a material risk of serious harm to individuals,

Duty / Prohibition

the system shall be classified as a high-impact system for the purposes of this Part, and the person responsible shall document and retain the basis for that classification in accordance with section 7.

Enforcement

The Minister may require production of classification records under sections 13 and 14, order an audit under section 15, require implementation of corrective measures under section 16, or order cessation under section 17 where misclassification gives rise to a serious risk of imminent harm.

B. Rationale

The current AIDA definition of "harm" is limited to physical, psychological, property, and economic loss to an individual. The amended clauses, including risk mitigation duties (s.8), monitoring obligations (s.9), notification of material harm (s.12), cessation powers for serious risk of imminent harm (s.17), publication powers (s.28), and criminal liability for serious harm (s.39), rely on a broader understanding of the types of impacts AI systems may cause. An expanded definition ensures that discriminatory, social, reputational, and collective harms are captured within the compliance and enforcement framework, preventing underinclusive application of the Act's mitigation, reporting, and penalty provisions.

3. Harm

A. Amendment

Subsection 5(1) of the Act is amended by replacing the definition of "harm" with the following:

Trigger

If the use, development, or deployment of an artificial intelligence system results in, or creates a material risk of, adverse impacts on individuals or groups,

Duty / Prohibition

"harm" shall include physical, psychological, economic, reputational, social, or discriminatory impacts, including cumulative or collective effects arising from the operation of the system.

Enforcement

The Minister, regulatory authority, or court shall apply this definition when assessing compliance under sections 8 to 12, issuing orders under sections 13 to 17, or imposing administrative or criminal penalties under sections 29, 30, and 39.

B. Rationale

The current definition of harm is limited to physical, property, and economic loss to an individual. The amendments expand oversight to include discriminatory impacts, systemic risk, monitoring obligations, incident reporting, and suspension powers. Because sections 8 (risk mitigation), 12 (notification of material harm), 17 (serious risk of imminent harm), and 39 (criminal liability) depend on how harm is understood, the definition must reflect social impacts.

4. Person Responsible

A. Amendment

Section 5(2) of the Act is amended by replacing subsection (2) with the following:

Trigger

If a person designs, develops, integrates, materially modifies, makes available for use, deploys, or manages the operation of an artificial intelligence system in the course of international or interprovincial trade and commerce, including where the system incorporates third-party models, components, or services,

Duty / Prohibition

that person shall be considered responsible for the system for the purposes of this Part, and responsibility shall not be avoided through contractual delegation, outsourcing, or reliance on external vendors.

Enforcement

The Minister may exercise powers under sections 13 to 17, require compliance with sections 6 to 12, and impose administrative monetary penalties or offences under sections 29 and 30 against any person meeting this definition.

B. Rationale

The current definition limits responsibility to those who design, develop, make available, or manage operation of a system, without clearly addressing integration of third-party components or downstream deployment. The amended clauses introduce expanded audit, monitoring, assessment, registration, and penalty obligations that must apply even where high-impact systems rely on external vendors or integrated models. A clarified definition ensures that compliance duties under sections 6–12, ministerial orders under sections 13–17, and penalties under sections 29–30 cannot be avoided through outsourcing or contractual structuring.

5. Regulated Activity

A. Amendment

Section 5(1) of the Act is amended by replacing the definition of "regulated activity" with the following:

Trigger

If a person, in the course of international or interprovincial trade and commerce, processes data for the purpose of training, testing, validating, deploying, integrating, materially modifying, monitoring, or operating an artificial intelligence system,

Duty / Prohibition

that activity shall constitute a regulated activity for the purposes of this Act, including activities involving third-party systems, integrated components, or post-deployment system updates.

Enforcement

Any person carrying out such activity is subject to the compliance obligations under sections 6 to 12, ministerial orders under sections 13 to 17, and administrative or criminal liability under sections 29, 30, and 39.

B. Rationale

The current definition focuses primarily on designing, developing, and making systems available, without clearly capturing deployment, integration, post-deployment modification, or ongoing monitoring. The amended clauses expand obligations related to audits, impact assessments, incident reporting, and enhanced penalties that apply throughout a system's lifecycle. A broader lifecycle-based definition ensures that compliance duties and enforcement powers apply not only at the design stage but also during deployment, modification, and operation, preventing regulatory gaps in post-deployment risk management.

6. Confidential Business Information

B. Amendment

Section 5(1) of the Act is amended by replacing the definition of "confidential business information" with the following:

Trigger

If information relates to the technical, financial, commercial, or operational affairs of a person and is claimed to be confidential in the context of compliance, audit, registry, publication, or enforcement under this Act,

Duty / Prohibition

the information shall be considered confidential business information only if it is not publicly available, reasonable measures have been taken to maintain its confidentiality, and its disclosure would result in material financial harm; however, information necessary to demonstrate compliance with sections 6 to 12, audit findings under section 15, or publication obligations under sections 11, 18, and 27 shall not be withheld solely on the basis of confidentiality where disclosure can be made in summarized or non-proprietary form.

Enforcement

The Minister may determine whether a claim of confidentiality is justified for the purposes of sections 22 to 28 and may require disclosure in redacted, aggregated, or abstracted form where necessary to enforce compliance.

C. Rationale

The current definition focuses solely on economic value and financial harm, without addressing the expanded transparency, registry, audit, and publication obligations introduced by the amended clauses. Because sections 11, 15, 18, 27, and 28 involve public disclosure and enforcement powers, the definition must balance legitimate protection of proprietary information with the need for regulatory transparency. Clarifying the scope of confidentiality prevents overbroad claims that could undermine audit authority, publication duties, or enforcement actions, while still protecting commercially sensitive information.

A. New Definitions

7. Risk

A. Amendment

Section 5(1) of the Act is amended by adding the following definition:

Trigger

If the Act refers to a risk of harm in relation to the design, development, deployment, or operation of an artificial intelligence system,

Duty / Prohibition

"risk" means the combination of the probability that harm will occur and the severity of that harm, including foreseeable and cumulative impacts.

Enforcement

The Minister, regulatory authority, or court shall apply this definition when exercising powers under sections 8, 12, 17, 28, 29, 30, and 39.

B. Rationale

The Artificial Intelligence and Data Act does not currently define "risk." However, the term is used implicitly in sections 8 (risks of harm), 12 (material harm), 17 (serious risk of imminent harm), and 28 (serious risk of imminent harm). The amended clauses expand enforcement and suspension powers based on risk thresholds. A statutory definition clarifies that risk involves both likelihood and severity, ensuring consistent application of mitigation, notification, audit, cessation, and penalty provisions.

8. Serious Harm

A. Amendment

Section 5(1) of the Act is amended by adding the following definition:

Trigger

If the Act refers to serious harm in relation to the use, development, deployment, or operation of an artificial intelligence system,

Duty / Prohibition

"serious harm" means harm that results in, or creates a material risk of, substantial physical, psychological, economic, or discriminatory impact on an individual or group, including harm occurring at scale or affecting fundamental interests.

Enforcement

The Minister, regulatory authority, or court shall apply this definition when exercising powers under sections 17, 28, 29, 30, and 39.

B. Rationale

The Act refers to "serious risk of imminent harm" (s.17, s.28) and imposes criminal liability where serious harm occurs (s.39), but does not define what makes harm "serious." The amended clauses strengthen suspension powers and escalated penalties that depend on seriousness thresholds. A statutory definition ensures consistent interpretation when determining cessation orders, public disclosure, administrative penalties, and criminal liability.

9. Incident

A. Amendment

Section 5(1) of the Act is amended by adding the following definition:

Trigger

If the Act requires notification, reporting, suspension, or enforcement action where an artificial intelligence system causes or is reasonably suspected of causing harm,

Duty / Prohibition

"incident" means an event or malfunction arising from the design, development, deployment, operation, or modification of an artificial intelligence system that results in, or creates a material risk of, serious harm, discriminatory impact, or systemic malfunction affecting individuals or groups.

Enforcement

The Minister or regulatory authority shall apply this definition when exercising powers under sections 12, 15, 17, 28, 29, and 30.

B. Rationale

The Act requires notification where use results or is likely to result in material harm (s.12) and authorizes audit and cessation orders where serious risk arises (ss.15–17), but it does not define the events that trigger these responses. The amended clauses expand reporting and suspension obligations tied to system failures or harmful outcomes. A definition of "incident" provides a clear threshold for when notification, investigation, audit, or enforcement mechanisms are activated, ensuring consistent application of oversight powers.

10. Independent Auditor

A. Amendment

Section 5(1) of the Act is amended by adding the following definition:

Trigger

If the Act requires or authorizes an audit to be conducted by an independent auditor under section 15,

Duty / Prohibition

"independent auditor" means a qualified third party who has no financial, operational, or decision-making conflict of interest in relation to the artificial intelligence system or the person responsible for it, and who meets any qualifications prescribed by regulation under subsection 15(2).

Enforcement

The Minister shall apply this definition when ordering or reviewing audits under section 15 and when assessing compliance with orders under section 16.

B. Rationale

Section 15 authorizes the Minister to require an audit and permits engagement of an independent auditor, but the Act does not define independence. Because the amended clauses expand audit obligations and strengthen enforcement consequences, the integrity of the audit process becomes central to compliance oversight. Defining "independent auditor" ensures that audits ordered under section 15 are conducted by impartial and qualified entities, preventing conflicts of interest that could undermine enforcement actions.

11. Material Modification

A. Amendment

Section 5(1) of the Act is amended by adding the following definition:

Trigger

If an artificial intelligence system is altered after its design, development, or initial deployment in a manner that may affect its purpose, performance, risk profile, or compliance obligations under this Act,

Duty / Prohibition

"material modification" means any change to the system's data, model parameters, architecture, deployment context, or operational logic that could reasonably affect the likelihood or severity of harm, the generation of biased output, or the system's classification as a high-impact system.

Enforcement

The Minister or regulatory authority may require reassessment under section 7, updated mitigation measures under sections 8 and 9, additional records under section 10, or an audit under section 15 where a material modification occurs.

B. Rationale

The Act imposes assessment, mitigation, monitoring, and record-keeping duties (ss.7–10) based on a system's risk profile, but it does not address how those duties apply when a system is updated or altered after deployment. The amended clauses introduce ongoing oversight and expanded enforcement mechanisms that must apply throughout a system's lifecycle. Defining "material modification" ensures that post-deployment changes triggering new risks cannot avoid reassessment, audit, or corrective action under sections 7–10 and 15–17.

12. Significant Decision

A. Amendment

Section 5(1) of the Act is amended by adding the following definition:

Trigger

If an individual is subject to a decision made, in whole or in part, by an artificial intelligence system in the course of a regulated activity,

Duty / Prohibition

"significant decision" means a decision that materially affects an individual's legal rights, access to employment, housing, credit, education, healthcare, essential services, economic interests, or other fundamental opportunities.

Enforcement

The Minister or regulatory authority shall apply this definition when assessing compliance with obligations relating to high-impact systems, audit requirements under section 15, mitigation duties under section 8, and administrative or criminal liability under sections 29, 30, and 39.

B. Rationale

The amended clauses introduce heightened obligations and oversight where AI systems materially affect individuals' access to fundamental opportunities. However, the Act does not define what types of decisions warrant enhanced scrutiny. A definition of "significant decision" establishes a clear threshold for when risk mitigation, monitoring, audit, and enforcement mechanisms should apply, ensuring consistent treatment of decisions with substantial legal or economic consequences.

13. Third-Party Component

A. Amendment

Section 5(1) of the Act is amended by adding the following definition:

Trigger

If a person responsible for an artificial intelligence system incorporates or relies on an external model, dataset, software module, scoring service, or other externally developed system in the design, development, deployment, or operation of that system,

Duty / Prohibition

"third-party component" means any model, dataset, software, service, or system developed or supplied by a separate legal person and integrated into or relied upon by an artificial intelligence system, whether directly or through contractual arrangement.

Enforcement

A person responsible for an artificial intelligence system that incorporates a third-party component remains subject to obligations under sections 6 to 12, ministerial orders under sections 13 to 17, and penalties under sections 29, 30, and 39, and may not avoid compliance duties on the basis that the component was developed externally.

B. Rationale

The Act assigns responsibility to persons who design, develop, make available, or manage AI systems, but does not address systems that rely on externally supplied models or components. The amended clauses expand audit, monitoring, impact assessment, and penalty obligations that must apply even where systems incorporate vendor-developed tools. Defining "third-party component" ensures that outsourcing or integration of external models does not create gaps in compliance or enforcement under sections 6–12 and 29–39.

APPENDIX B
AMENDMENTS TO ENFORCEMENT AND INSTITUTIONAL POWERS

Amendment to Section 28

28(3) Where a person is found to have committed a violation under this Act or is convicted of an offence under this Act, the Minister shall publish, on a publicly available website,

(a) the name of the corporation responsible or, in the case of an individual, where publication is proportionate;

(b) the nature of the violation or offence;

(c) the penalty imposed; and

(d) any compliance measures ordered.

28(4) Publication under subsection (3) shall not include personal information or confidential business information beyond what is necessary to ensure public accountability.

Amendment to Section 29

29(5) A person or corporation that contravenes sections 6 to 12 of this Act is liable to an administrative monetary penalty not exceeding

(a) a prescribed percentage of the person's gross global revenue in the preceding financial year; or

(b) a prescribed maximum monetary amount,

whichever is greater.

29(6) In determining the amount of a penalty, the following factors shall be considered:

(a) the severity and duration of the violation;

(b) the degree of intent, recklessness or negligence;

(c) the level of actual or potential harm;

(d) any history of previous violations under this Act; and

(e) measures taken to mitigate or remedy the violation.

Amendment to Section 30

30(6) Where a person commits a second or subsequent offence under this Act within five years of a prior conviction, the maximum fine otherwise applicable shall be increased by up to 50 percent.

30(7) In determining sentence for a repeat offence, the court shall consider:

(a) the pattern of non-compliance;

(b) the adequacy of prior penalties;

(c) whether corrective measures were implemented following the earlier conviction.

30(8) A conviction entered within five years prior to the commission of a subsequent offence constitutes a prior conviction for the purposes of this section.

Amendment to Section 32

32(d) require regulated organizations to submit periodic compliance reports relating to high-impact artificial intelligence systems;

32(e) require submission of information necessary to evaluate systemic risks and patterns of non-compliance;

32(f) issue binding compliance guidelines and risk mitigation standards where systemic risks are identified.

Amendment to Section 33

33(1) The Governor in Council shall appoint an Artificial Intelligence and Data Commissioner to act independently in the administration and enforcement of this Part.

33(2) The Commissioner shall hold office for a fixed term and may be removed only for cause.

33(3) The Commissioner shall submit an annual report to Parliament on enforcement activities, compliance patterns, and systemic risk findings under this Part.

Amendment to Section 34

34(2) An analyst designated under this section shall possess the necessary technical, legal, or regulatory expertise in artificial intelligence systems.

34(3) An analyst shall act independently and shall not hold any financial or operational interest in an artificial intelligence system subject to review.

34(4) Analysts shall be bound by confidentiality and conflict-of-interest obligations prescribed by regulation.

Amendment to Section 35

35(4) The advisory committee shall include members with demonstrated expertise in artificial intelligence, ethics, human rights, privacy, and technological governance.

35(5) The Minister shall ensure diversity of background and independence among committee members.

35(6) Advice and recommendations of the committee shall be published on a publicly available website, subject to confidentiality safeguards.

Amendment to Section 36

36(1.1) Before making regulations under this Part, the Governor in Council shall publish draft regulations for public consultation.

36(1.2) Regulations shall be tabled before Parliament prior to coming into force.

36(1.3) In making regulations, the Governor in Council shall consider impacts on innovation, fundamental rights, and protection of individuals from harm.

Amendment to Section 38

38(1) Every person commits an offence if the person possesses or uses personal information that they knew or ought reasonably to have known was obtained unlawfully.

38(2) Where a person is found in violation of subsection (1), the court may order:

(a) deletion of unlawfully obtained personal information;

(b) suspension of development or deployment of the artificial intelligence system until compliance is achieved;

(c) implementation of improved due diligence and data governance measures.

Amendment to Section 39

39(1) A person commits an offence where they knowingly, recklessly, or through clear negligence make available an artificial intelligence system whose design or deployment carries a significant and reasonably foreseeable risk of serious harm.

39(2) Liability under this section may arise whether or not actual harm was intended, where such harm was reasonably foreseeable.

Amendment to Section 40

40(3) In addition to any penalty imposed under this section, the court may order:

(a) restriction or prohibition of operation of the system involved;

(b) implementation of specific compliance measures within a prescribed period;

(c) mandatory independent third-party auditing;

(d) periodic reporting to the appropriate regulatory authority.

Appendix C
New sections

Automated Decision Systems Involving Personal Information: The following section is added after section 8:

8.1 (1) Where a regulated activity involves the use of an artificial intelligence system that makes or materially influences a significant decision affecting an individual, the person responsible shall ensure that:

(a) the use of the system is demonstrably necessary and proportionate to the identified purpose;

(b) the personal information processed is limited to what is reasonably required for that purpose;

(c) appropriate safeguards are implemented to mitigate risks of bias, inaccuracy, or unfair outcomes; and

(d) individuals are informed, in clear and plain language, of the use of such systems where they may materially affect them.

Completeness of Transparency Response: The following section is added after section 11:

11.1 (1) Where an individual requests information relating to the use of a high-impact system affecting them, the person responsible shall respond with due diligence and not later than thirty days from receipt of the request.

(2) A response under subsection (1) is complete if it provides access to all information under the control of the person responsible that is relevant to the individual's interaction with the system, subject only to lawful exceptions.

Severability and Derived Data Obligations: The following section is added after section 11.1:

11.2 (1) For the purposes of providing information relating to a high-impact system, information relating to a third party is reasonably severable if:

(a) it can be removed, redacted, or anonymized without materially distorting the meaning of the remaining information; and

(b) its removal does not render the remaining information misleading or unintelligible to a reasonable person.

(2) Where a person responsible determines that information is not reasonably severable, they shall document the basis for that determination and provide the individual with a written explanation of the refusal.

(3) Where personal information relating to an individual has been used to generate derived data, inferences, profiles, or predictive outputs, including for the purpose of training, testing, validating, or refining an artificial intelligence system, the person responsible shall: