An Autopsy of Ambition: A Deep Dive into Canada's Bill C-27 and its Unfinished Digital Legacy

Executive Summary

Bill C-27, the *Digital Charter Implementation Act, 2022*, represented the Canadian federal government's most ambitious attempt to modernize its legal framework for the digital age. Tabled in the House of Commons on June 16, 2022, the omnibus bill aimed to overhaul private-sector privacy law, which had been governed by the increasingly obsolete *Personal Information Protection and Electronic Documents Act* (PIPEDA), and to introduce a novel regulatory regime for artificial intelligence (AI). However, after a protracted and contentious journey through the legislative process, including extensive study by the Standing Committee on Industry and Technology (INDU), the bill died on the Order Paper when Parliament was prorogued on January 6, 2025. This report provides an exhaustive analysis of Bill C-27, deconstructing its components, evaluating its objectives, and synthesizing the multifaceted debates that defined its consideration.

The legislation was composed of three distinct acts. The *Consumer Privacy Protection Act* (CPPA) was designed to replace PIPEDA's privacy provisions, introducing new individual rights such as data portability and erasure, stricter consent requirements, and significantly higher financial penalties for non-compliance. The *Personal Information and Data Protection Tribunal Act* (PIDPTA) proposed a new administrative tribunal to hear appeals from the Privacy Commissioner of Canada and impose penalties, a structural choice that drew significant criticism for potentially weakening enforcement. Finally, the *Artificial Intelligence and Data Act* (AIDA) was Canada's first legislative foray into regulating AI, establishing a risk-based framework for "high-impact" systems.

During its review, Bill C-27 was the subject of intense scrutiny from a wide spectrum of stakeholders. Civil society organizations and privacy advocates argued for the enshrinement of privacy as a fundamental right within the operative text of the law, not just its preamble, and criticized exceptions to consent, such as the "legitimate interest" clause, as overly broad. Corporate stakeholders, while supportive of modernization, raised concerns about the need

for legal clarity, harmonization with provincial and international standards like Quebec's Law 25 and the EU's GDPR, and the potential for new rules to stifle innovation. The Office of the Privacy Commissioner (OPC) itself was a key critic, advocating for direct order-making and fining powers rather than the proposed two-step process involving the PIDPTA.

The AIDA component of the bill was particularly controversial, facing near-universal calls for it to be severed from the privacy legislation to allow for more thorough consultation. Its initial vagueness and reliance on future regulations were seen as critical flaws. In response, the government tabled substantial amendments mid-way through the committee process, seeking to define "high-impact" systems and clarify obligations. While these changes were intended to address criticism, they were viewed by many as a reactive measure that underscored the bill's premature drafting.

Ultimately, the prorogation of Parliament terminated the bill's progress, leaving Canada's federal privacy laws unmodernized. Despite its failure, Bill C-27's legacy is significant. It has indelibly shaped the national conversation on digital policy, establishing a new baseline for expected consumer rights and corporate accountability. The extensive testimony and debate it generated will serve as a critical resource for future legislative efforts, which will inevitably have to grapple with the same contentious issues: the legal status of privacy, the optimal structure for regulatory enforcement, and the immense challenge of crafting effective, rights-respecting legislation for artificial intelligence. The next iteration of digital reform in Canada will likely see AI regulation treated in a standalone bill, a direct lesson learned from the troubled journey of Bill C-27.

1. Introduction: The Imperative for Digital Reform in Canada

1.1 The Obsolescence of PIPEDA in the Age of Big Data and AI

Canada's federal private-sector privacy law, the *Personal Information Protection and Electronic Documents Act* (PIPEDA), was enacted in 2000, a time when the digital economy was in its infancy. It was designed for a world of nascent e-commerce, not one dominated by the ubiquitous data collection, algorithmic processing, and artificial intelligence systems that define the contemporary landscape.[1] Over two decades, the exponential growth of data, the rise of global social media platforms, and the rapid advancement of AI have rendered PIPEDA's framework fundamentally outdated.[2] The Act's enforcement model, which relied

heavily on the Privacy Commissioner's power to investigate and recommend rather than issue binding orders or levy significant fines, was widely seen as insufficient to hold powerful global technology companies accountable. This legislative gap created an urgent need for modernization to restore consumer trust, give Canadians meaningful control over their personal information, and foster an environment of responsible innovation.[3]

1.2 The Genesis of Bill C-27: From the Digital Charter to Legislative Action

The policy groundwork for Bill C-27 was laid in 2019 with the unveiling of Canada's Digital Charter. This initiative, born from extensive national consultations, established ten core principles intended to guide Canada's approach to the digital world.[4] Key principles such as "Control and Consent," "Transparency, Portability and Interoperability," and "Strong Enforcement and Real Accountability" directly informed the subsequent legislative push.[5] Bill C-27, officially titled the *Digital Charter Implementation Act, 2022*, was the government's concrete attempt to translate these high-level principles into enforceable law.[6]

This was not the government's first attempt at reform. Bill C-27 incorporated and expanded upon a previous legislative effort, Bill C-11, which was introduced in 2020 but died on the Order Paper when a general election was called in 2021.[4] The reintroduction of these reforms as Bill C-27 signaled a sustained commitment from the government to address the pressing need for a modernized digital policy framework.

1.3 Overview of the Bill's Tripartite Structure and Legislative Journey

Bill C-27 was an omnibus bill composed of three separate but interconnected proposed acts, each tackling a different facet of digital governance.[1]

1. **The Consumer Privacy Protection Act (CPPA):** The core of the bill, designed to repeal and replace the privacy provisions of PIPEDA with a new, more robust regime for the protection of personal information in the course of commercial activities.[13]
2. **The Personal Information and Data Protection Tribunal Act (PIDPTA):** A new act that would establish a specialized administrative tribunal to review decisions of the Privacy Commissioner and impose financial penalties.[11]
3. **The Artificial Intelligence and Data Act (AIDA):** A groundbreaking piece of legislation that aimed to create Canada's first legal framework for the regulation of AI systems.[15]

The bill was introduced in the House of Commons on June 16, 2022.[15] After several rounds of debate, it passed its second reading on April 24, 2023, with a vote of 205 to 109, and was subsequently referred to the Standing Committee on Industry and Technology (INDU) for detailed study.[3] The INDU committee conducted extensive hearings from September 2023 through May 2024, hearing from over 100 witnesses and receiving dozens of written briefs.[7] However, the bill's legislative journey was cut short. On January 6, 2025, Parliament was prorogued, a constitutional procedure that ends a parliamentary session and terminates all outstanding legislative business. As a result, Bill C-27 died on the Order Paper, failing to become law.[7]

2. Part I: Deconstructing the Consumer Privacy Protection Act (CPPA)

The CPPA formed the centerpiece of Bill C-27, representing a comprehensive overhaul of Canada's private-sector privacy rules. It aimed to replace the core of PIPEDA with a modernized framework that enhanced individual rights, clarified organizational responsibilities, and introduced a significantly more stringent enforcement regime.

2.1 Modernizing Consent and Transparency

While the CPPA maintained PIPEDA's foundational consent-based model, it sought to elevate the standard for what constitutes valid consent. A key requirement was that organizations provide individuals with specific information in "plain language" at or before the time of collection.[10] This information had to include the purposes for collection, use, and disclosure; the manner in which it would be handled; the specific types of personal information involved; the names or types of any third parties with whom it would be shared; and any reasonably foreseeable consequences of the collection, use, or disclosure.[10]

The Act established "express consent" as the default requirement for the collection, use, and disclosure of personal information.[10] However, it allowed for "implied consent" to be considered appropriate in certain circumstances, based on an evaluation of the individual's reasonable expectations and the sensitivity of the information in question.[10] This distinction aimed to provide organizations with a degree of flexibility while ensuring that more sensitive activities required a clear, affirmative action from the individual.

2.2 New Individual Rights

A cornerstone of the CPPA was the introduction of new rights for individuals, designed to give them greater control over their personal information in the digital ecosystem. These rights were largely inspired by international frameworks like the GDPR and were intended to address the power imbalance between individuals and data-driven organizations.

2.2.1 Right to Disposal (Erasure)

The CPPA created a statutory right for individuals to request that an organization dispose of their personal information.[4] Organizations would be required to comply with such a request, subject to a number of exceptions. These exceptions included situations where retaining the information was required by law, where it was necessary for a legal claim, or where it was subject to a contractual or legal retention period.[24] This right was particularly contentious. The Office of the Privacy Commissioner, in its submission to the INDU committee, raised a significant concern that one of the exceptions—allowing an organization to refuse disposal if the information was scheduled to be disposed of according to a pre-existing retention policy—could render the right practically ineffective for many individuals, creating a loophole that would permit continued retention against an individual's wishes.[25]

2.2.2 Right to Data Portability (Mobility)

To promote competition and empower consumers, the CPPA introduced a right to data portability.[4] This right would allow an individual to direct an organization to transfer their personal information to another designated organization in a secure format. This process was to be governed by a "data mobility framework" to be established through future regulations.[4] The intent was to reduce friction for consumers wishing to switch service providers, for example, from one social media platform or financial institution to another, thereby fostering a more competitive digital marketplace.[2]

2.2.3 Right to Algorithmic Transparency

Addressing the growing use of automated systems in decision-making, the CPPA established a right to an explanation.[1] If an organization used an automated decision system to make a prediction, recommendation, or decision about an individual that could have a "significant impact" on them, the individual had the right to request an explanation of how that decision was made. The organization would be required to provide a plain-language account of the main factors that led to the decision, a provision aimed at demystifying the "black box" of algorithmic processing.

2.3 Organizational Accountability

The CPPA moved beyond PIPEDA's principles-based approach to impose more concrete and demonstrable accountability obligations on organizations.

2.3.1 Privacy Management Programs

A central requirement of the CPPA was that every organization must implement and maintain a comprehensive privacy management program.[2] This program was required to include the policies, practices, and procedures the organization put in place to fulfill its obligations under the Act. This included processes for protecting personal information, handling access requests and complaints, providing training to staff, and developing public-facing materials explaining its privacy practices. The Privacy Commissioner would have the power to request and review these programs to assess compliance.

2.3.2 De-identification and Anonymization

The CPPA introduced, for the first time in federal law, distinct statutory definitions for "de-identify" and "anonymize," resolving an ambiguity that had been a point of criticism in the previous Bill C-11.[24]

- **De-identify** was defined as modifying personal information so that an individual cannot be *directly* identified, though a risk of re-identification remains.[24] De-identified information would still be considered personal information and thus remain subject to the

Act's protections.
- **Anonymize** was defined as irreversibly and permanently modifying personal information, in accordance with generally accepted best practices, to ensure that no individual can be identified, whether directly or indirectly, by any means.[12] Truly anonymized information would fall outside the scope of the Act.

This distinction was crucial, but the high bar set for anonymization—requiring an irreversible and permanent modification against *any means* of re-identification—was a significant point of contention for industry stakeholders. Groups like the Canadian Life and Health Insurance Association and the Canadian Chamber of Commerce argued that this absolute standard was practically impossible to achieve and called for a more flexible "reasonableness" standard, similar to that found in Quebec's Law 25.[27]

2.4 Special Protections for Minors

Recognizing the particular vulnerability of children in the digital environment, the CPPA introduced specific and heightened protections for their data. The Act explicitly designated the personal information of minors as "sensitive information" by default.[3] This classification automatically triggered a higher standard of care and more stringent consent requirements for any organization handling such data. Furthermore, the right to disposal was more expansive for minors, with fewer exceptions, granting them and their guardians greater power to have their digital footprint erased.[24]

Despite these improvements, child-focused organizations like UNICEF Canada argued the bill could go further. In their brief to the INDU committee, they recommended that the government conduct a formal Child Rights Impact Assessment and explicitly incorporate the "Best Interests of the Child"—a well-established principle from the UN Convention on the Rights of the Child—as a guiding principle within the Act itself.[6] This recommendation was later echoed by the Privacy Commissioner, who suggested this specific legal terminology would be more robust than the government's proposed language of "special interests of minors".[25]

2.5 Exceptions to Consent: The "Legitimate Interest" Controversy

One of the most significant and debated changes in the CPPA was the introduction of new exceptions to the requirement to obtain consent. The most notable of these was the

"legitimate interest" exception, which would permit an organization to collect or use personal information without consent if it could demonstrate that it had a legitimate interest that outweighed any potential adverse effect on the individual.[10] This exception was subject to two key conditions: the activity must be one that a reasonable person would expect, and the information could not be collected or used for the purpose of influencing the individual's behaviour or decisions.[4]

The inclusion of this concept was a clear attempt to align the CPPA with the language of the EU's GDPR, which includes "legitimate interests" as a lawful basis for processing data. However, the implementation in the Canadian context created a structural difference with profound implications. In the GDPR, "legitimate interests" is one of six distinct and co-equal lawful bases for processing; it is an alternative to consent, to be used when consent may not be the most appropriate foundation. In the CPPA, by contrast, it was framed as an *exception* to a regime where consent remained the primary rule.[10]

This subtle but critical distinction created what many critics saw as a significant structural weakness. It raised the possibility that organizations could effectively have it both ways. They could first rely on a weak form of "implied consent," often buried in lengthy terms of service that users do not read. If that was challenged, they could then fall back on the "legitimate interest" exception, which relied on an internal risk assessment conducted by the business itself, rather than a rights-based judgment.[29] This mechanism appeared to be in direct tension with the bill's stated purpose of enhancing individual "control and consent".[5] By creating a pathway to bypass meaningful consent, the clause risked weakening the very protections it was meant to modernize, potentially eroding public trust rather than strengthening it.

3. Part II: A New Adjudicative Body: The Personal Information and Data Protection Tribunal Act (PIDPTA)

The second component of Bill C-27, the *Personal Information and Data Protection Tribunal Act*, proposed the creation of a new administrative body to oversee the enforcement of the CPPA. This represented a significant departure from the existing enforcement model under PIPEDA and became one of the most heavily criticized aspects of the bill.

3.1 Mandate, Jurisdiction, and Composition

The PIDPTA would establish the Personal Information and Data Protection Tribunal, a quasi-judicial body with a narrowly defined and limited jurisdiction.[1] Its primary functions were twofold:

1. To hear appeals of certain decisions, findings, and compliance orders issued by the Privacy Commissioner of Canada under the CPPA.
2. To review recommendations from the Privacy Commissioner to impose administrative monetary penalties (AMPs) and to make the final decision on whether to levy a penalty and in what amount.[3]

The Tribunal was to be composed of three to six members appointed by the Governor in Council, with a requirement that at least three members must have demonstrated experience in the field of information and privacy law.[1] Its decisions would be final and binding, subject only to judicial review by the Federal Court of Appeal on limited grounds.[4]

3.2 The Adjudicative Model and Stakeholder Critiques

The government's stated rationale for creating the Tribunal was to provide an accessible and specialized mechanism for organizations and individuals to seek a review of the Privacy Commissioner's decisions, thereby creating a check on the regulator's new and expanded powers.[8] However, this model was met with strong and persistent opposition from the Privacy Commissioner himself, as well as from numerous privacy advocates and opposition parties.

The core criticism, articulated forcefully by Privacy Commissioner Philippe Dufresne in his testimony before the INDU committee, was that the Tribunal introduced an unnecessary and cumbersome layer of bureaucracy into the enforcement process.[25] He argued that it would inevitably lead to delays, making it more difficult and expensive for individuals to see their privacy rights vindicated.[25] The Commissioner pointed out that none of his provincial counterparts, who possess direct order-making and fining powers, operate under such a two-tiered system; in those jurisdictions, appeals of the regulator's decisions go directly to the courts.[25] This critique was echoed by privacy advocates and the Conservative Party, who argued that the model fundamentally weakened the Office of the Privacy Commissioner by denying it the direct authority to enforce its own findings, a power seen as essential for a modern and effective regulator.[3]

This debate over the Tribunal's existence exposed a fundamental flaw in the bill's enforcement architecture. The government actively promoted Bill C-27 by highlighting its "strong enforcement and real accountability" and boasting that it would create the "strongest fines among G7 privacy laws".[5] Yet, the mechanism designed to deliver this strong enforcement was bifurcated and indirect. The Privacy Commissioner, as the expert investigative body, could

only *recommend* a penalty to the Tribunal, which would then re-adjudicate the matter before deciding whether to impose the fine.[10]

This separation of the investigative and punitive functions represents a significant dilution of regulatory power compared to international models like the GDPR, where data protection authorities can investigate and directly levy fines. A regulator's ability to impose a direct and swift penalty is a far more potent deterrent to non-compliance than the ability to recommend a penalty that will be subject to a second, potentially lengthy and costly, adjudicative process. The very structure of the PIDPTA, conceived as a safeguard, risked undermining the bill's central promise of "real accountability" by making the path to penalties longer, more complex, and less certain.

4. Part III: Canada's Inaugural AI Legislation: The Artificial Intelligence and Data Act (AIDA)

The third and most novel part of Bill C-27 was the *Artificial Intelligence and Data Act* (AIDA). It represented Canada's first legislative attempt to establish a comprehensive regulatory framework for the development and deployment of AI systems, positioning Canada alongside the European Union as a first-mover in this complex policy domain.[1]

4.1 A Risk-Based Approach: Regulating "High-Impact" AI Systems

AIDA was designed around a risk-based approach, focusing its most stringent obligations on what it termed "high-impact systems".[3] This approach mirrored the tiered framework of the EU's AI Act, which tailors regulatory burdens to the level of risk a system poses to health, safety, and fundamental rights.[1]

In its original form, the bill was heavily criticized because it did not define what constituted a "high-impact system" in the legislative text itself. Instead, it delegated this crucial determination to future regulations to be developed by the government.[2] This lack of clarity created significant uncertainty for businesses and was a major focus of stakeholder concern. Those persons responsible for a system deemed to be high-impact would be subject to a suite of obligations, including assessing and mitigating risks of harm and biased output, establishing measures for monitoring the system's performance, maintaining detailed records,

and publishing a plain-language description of the system's purpose and capabilities.[4]

4.2 Prohibitions, Penalties, and the AI and Data Commissioner

AIDA established several key prohibitions. It would make it an offence to process or use illegally obtained personal information for the purpose of designing, developing, or deploying an AI system.[3] It also prohibited knowingly or recklessly making an AI system available for use if its use was likely to cause, or did cause, serious physical or psychological harm to an individual or substantial damage to their property.[11]

To oversee this new regime, the Act provided for the appointment of an AI and Data Commissioner. This new official would be housed within the department of Innovation, Science and Economic Development Canada (ISED) and would be tasked with supporting the Minister in the administration and enforcement of the Act, including monitoring compliance and ordering third-party audits.[4]

4.3 The Evolution of AIDA: Substantive Government Amendments

Faced with a barrage of criticism regarding AIDA's vagueness and the extensive delegation of power to the executive branch, the Minister of Innovation, Science and Industry tabled a set of comprehensive amendments in late 2023, while the bill was under review by the INDU committee.[31] These amendments were so substantial that some stakeholders, including the Canadian Chamber of Commerce, argued they effectively created a "fundamentally new piece of legislation".[19]

The key proposed changes included [36]:

- **A New Definition of AI:** The amendments proposed a new, clearer definition of "artificial intelligence system" that was aligned with the one developed by the Organisation for Economic Co-operation and Development (OECD), moving away from a technology-specific definition to a more principles-based one.
- **Defining "High-Impact" in the Act:** In a direct response to the most significant criticism, the amendments proposed to write an initial list of seven classes of "high-impact systems" directly into the legislation. These classes covered sensitive areas such as employment decisions, the provision of services, biometric information processing, content moderation on online platforms, healthcare, decision-making by courts or administrative bodies, and law enforcement.

- **Clarifying the AI Value Chain:** The amendments sought to establish more distinct and delineated responsibilities for different actors across the AI lifecycle, including developers of machine-learning models, developers of high-impact systems, and those who manage the operation of such systems.
- **Regulating General-Purpose AI:** New obligations were introduced for developers of "general-purpose AI systems" (such as large language models), including requirements to assess and mitigate risks and to ensure transparency.
- **Strengthening the Commissioner's Role:** The amendments proposed to entrench the role of the AI and Data Commissioner more firmly in the statute and grant them new powers, including the authority to compel the production of accountability frameworks and to conduct audits.

The process by which AIDA was developed and amended reveals a great deal about the challenges of legislating on rapidly emerging technologies. The bill was met with widespread and forceful criticism from its inception by a diverse array of stakeholders, including civil society groups, industry associations, and academic experts, for being underdeveloped, lacking meaningful public consultation, and concentrating too much power within the Minister's office.[28] The government's decision to introduce transformative amendments mid-way through the committee process, rather than withdrawing the bill for further development, was a reactive strategy that did little to build stakeholder confidence.

This legislative approach suggests that the government was attempting to "build the plane while flying it." The near-unanimous call from stakeholders to sever AIDA from the privacy reforms in Bill C-27 underscores the perception that it was not ready for legislative debate.[28] This experience serves as a powerful case study. It suggests that for novel and complex technological domains like AI, the traditional legislative drafting process may be insufficient. A more effective path forward might involve a more collaborative and expert-driven pre-legislative phase, such as a dedicated commission or public inquiry, to build consensus and establish a solid policy foundation before a bill is ever tabled in Parliament. The troubled genesis of AIDA highlights the perils of legislating on emerging technology without first doing that foundational work.

5. Part IV: The Crucible of Debate: A Thematic Analysis of Stakeholder Testimony from INDU Hearings

The hearings of the Standing Committee on Industry and Technology (INDU) on Bill C-27 became the central forum for a national debate on the future of digital rights and regulation in Canada. The testimony and written briefs submitted by dozens of organizations revealed deep divisions and fundamental disagreements on the bill's core principles and mechanisms. A

thematic analysis of this record provides a clear picture of the key battlegrounds that defined the bill's journey.

5.1 Theme 1: The Status of Privacy as a Fundamental Right

A primary point of contention was the legal status of privacy. While the preamble to Bill C-27 recognized that privacy is "essential to individual autonomy and dignity and to the full enjoyment of fundamental rights and freedoms," this was not sufficient for many advocates.[39]

- **Civil Society Position:** Groups such as the International Civil Liberties Monitoring Group and the BC Civil Liberties Association argued passionately that placing this recognition only in the non-binding preamble was a critical flaw. They contended that privacy must be explicitly defined as a fundamental right within the operative, enforceable text of the Act. This, they argued, was necessary to ensure that in any conflict, privacy rights would be given proper legal weight and not simply "balanced" away against competing commercial interests.[38]
- **Government Response:** In response to this pressure, the government proposed an amendment to add the recognition of privacy as a fundamental right to the CPPA's purpose clause (section 5).[33] While seen as a positive step, it still fell short of the more robust enshrinement in the body of the Act that civil society groups had demanded.
- **Analysis:** This debate exposed a core philosophical tension running through the entire bill. It raised the question of whether the legislation was fundamentally a consumer protection statute, designed to manage the relationship between businesses and customers by balancing their respective interests, or a human rights instrument, designed to protect a fundamental right from encroachment. The government's approach attempted to bridge this divide, but for many rights advocates, it failed to provide the unequivocal prioritization that a fundamental right requires.

5.2 Theme 2: The Efficacy of the Enforcement Model

The proposed enforcement structure, centered on the new Personal Information and Data Protection Tribunal, was heavily criticized for being inefficient and weak.

- **OPC's Position:** The Privacy Commissioner was the most prominent critic of this model. Commissioner Dufresne's testimony consistently highlighted that the PIDPTA would act as an unnecessary intermediary, delaying justice for complainants and adding costs to the system.[25] He advocated for the OPC to be granted direct order-making and fining

powers, which would align the federal regime with its provincial counterparts and provide for swifter, more decisive enforcement.[25]

- **Private Right of Action (PRA):** The bill proposed a new private right of action, allowing individuals to sue for damages for a privacy violation. However, this right was contingent on the OPC or the Tribunal first making a formal finding of contravention. The OPC argued that this prerequisite would create a significant bottleneck, as their office could not possibly investigate every complaint to the point of a formal finding. They recommended that the right to sue should be triggered by the filing of a complaint with their office, but not dependent on its final outcome, thereby opening a more direct path to the courts for individuals seeking remedy.[25]
- **Analysis:** This theme revealed a profound disagreement on the proper architecture of regulatory power. The government's model prioritized checks and balances, creating a separation between the investigative function (OPC) and the adjudicative/penalty function (PIDPTA). Critics, however, saw this separation not as a safeguard but as a deliberate weakening of the regulator, arguing that an effective data protection authority must have the power to enforce its own findings directly.

5.3 Theme 3: Balancing Innovation and Individual Protection

The central tension in any data protection law—the balance between protecting personal information and allowing for its use in commercial and innovative activities—was a constant theme throughout the hearings.

- **Corporate Perspective:** Industry representatives consistently argued for greater flexibility and clarity to avoid stifling innovation and imposing undue compliance burdens. Key recommendations from groups like Meta, Rogers Communications, the Canadian Chamber of Commerce, and the Canadian Life and Health Insurance Association included [27]:
  - Adopting a "reasonableness" standard for anonymization, arguing the proposed definition was unattainable.
  - Broadening the exceptions to consent for "business activities" and for internal research and development.
  - Implementing a phased, multi-year transition period to allow businesses, particularly small and medium-sized enterprises (SMEs), to adapt to the new rules.
  - Concerns that AIDA's scope was overly broad, particularly its classification of systems like content moderation as "high-impact," which they argued would impose disproportionate obligations.
- **Civil Society Counterpoint:** In contrast, many academics and civil liberties advocates argued that the bill was already tilted too far in favor of commercial interests. They pointed to the "legitimate interest" exception as a prime example of a provision that

prioritized business flexibility over meaningful individual consent.[29] Their view was that the bill's framing of privacy as a consumer issue to be balanced against economic goals was fundamentally flawed and that human rights should not be subject to a cost-benefit analysis.

- **Analysis:** The testimony on this theme vividly illustrates the chasm between the business community's desire for legal certainty and operational latitude, and civil society's demand for a robust, rights-centric framework. The bill's drafters attempted to find a middle ground, but in doing so, they often failed to fully satisfy either side.

5.4 Theme 4: The Protection of Vulnerable Groups and Collective Harms

A more sophisticated critique of the bill emerged from witnesses who argued that its focus on individual data transactions and consumer harm was inadequate to address the systemic and collective impacts of the data economy.

- **Children's Privacy:** While the bill included enhanced protections for minors, organizations like UNICEF and the University of Ottawa's CIPPIC clinic argued for a more comprehensive, rights-based approach. They called for the adoption of the "best interests of the child" principle as the explicit legal standard, a measure that would require organizations to proactively design their services with child safety and well-being as a primary consideration.[6]
- **Group and Intersectional Harms:** A powerful submission from a group of communications and privacy scholars argued that the bill was blind to the ways in which data processing and AI systems can inflict collective and discriminatory harms on already marginalized communities.[43] They pointed to examples like biased algorithms in hiring or insurance that perpetuate systemic inequalities. They called for the bill to be amended to include an "intersectional lens," requiring consideration of group-based harms and not just individual privacy violations.
- **Analysis:** This line of testimony represents a crucial evolution in the public understanding of privacy. It moves the conversation beyond a narrow focus on individual control over personal data to a broader consideration of data justice and the societal impacts of algorithmic systems. The fact that Bill C-27 was largely unequipped to address these collective, discriminatory harms was seen as a significant shortcoming.

5.5 Theme 5: The Viability of AIDA

Perhaps the most striking area of consensus to emerge from the hearings was the widespread opposition to the *Artificial Intelligence and Data Act* in its current form and as part of this specific bill.

- **A Call for Separation:** A diverse coalition of stakeholders, from the Canadian Chamber of Commerce on the industry side to the BC Civil Liberties Association on the rights-advocacy side, united in their recommendation to sever AIDA from the rest of Bill C-27.[28]
- **Rationale:** The reasoning was remarkably consistent across these otherwise disparate groups. AIDA was seen as a rushed and underdeveloped piece of legislation that lacked the necessary foundation of expert and public consultation. Its heavy reliance on future regulations created massive uncertainty, and its complexity was seen as a threat to the timely passage of the urgently needed privacy updates in the CPPA.[28]
- **Expert Critique:** Prominent AI experts and digital governance advocates were among AIDA's harshest critics. Bianca Wylie, for instance, argued for scrapping the legislation entirely and starting over with an adaptive, sector-specific regulatory approach, rather than attempting a one-size-fits-all law that would be unable to account for the contextual nature of AI-driven harms.[34]
- **Analysis:** The broad-based opposition to AIDA's inclusion in Bill C-27 was arguably the single greatest political impediment the bill faced during its committee study. It sent a clear signal that while there was an appetite for AI regulation, the approach taken in AIDA was deeply flawed and its premature inclusion in an already complex privacy bill was a critical strategic error.

6. Part V: Comparative Legal Analysis: C-27 in a Global Context

Bill C-27 was not drafted in a vacuum. It was a direct response to a rapidly evolving international and domestic landscape of data protection law. Its success or failure, particularly in the eyes of the business community and international partners, depended heavily on its alignment with two key benchmarks: the European Union's *General Data Protection Regulation* (GDPR) and Quebec's Law 25.

6.1 Benchmarking Against the Gold Standard: Alignment with the EU's GDPR

A primary objective of the Canadian government in drafting Bill C-27 was to ensure that Canada would maintain its "adequacy" status with the European Union.[3] An adequacy decision from the European Commission allows for the free flow of personal data from the EU to a third country without the need for additional safeguards, a critical facilitator for transatlantic trade.[45] Therefore, aligning the CPPA with the principles of the GDPR was a key design consideration.

The bill showed clear points of convergence with the GDPR, such as the introduction of a right to data portability, the right to erasure (disposal), the emphasis on privacy management programs, and the introduction of significant financial penalties.[46] However, there were also crucial areas of divergence that raised questions about the true extent of its alignment:

- **Basis for Processing:** As previously analyzed, the CPPA's treatment of "legitimate interest" as an *exception* to consent, rather than a co-equal lawful basis, was a significant departure from the GDPR's structure.[29]
- **Enforcement Model:** The CPPA's two-step enforcement process, requiring the OPC to make recommendations to the PIDPTA, stood in stark contrast to the GDPR's model, which grants Data Protection Authorities (DPAs) the direct power to investigate and impose fines.[25]
- **Data Transfers:** The CPPA's requirements for international data transfers were less prescriptive than those under the GDPR. The CPPA required an organization to ensure, by contract or other means, an "equivalent" level of protection when transferring data to a service provider, but it lacked the more detailed mechanisms and adequacy requirements of the European framework.[29]

6.2 The Domestic Counterpart: A Comparative Review Against Quebec's Law 25

While Bill C-27 was being debated in Ottawa, Quebec's comprehensive privacy reform, known as Law 25, was coming into force in stages. This made Law 25 the de facto highest standard for privacy protection in Canada and a crucial domestic benchmark for the federal bill.[22] Inter-provincial harmonization was a key goal for many business stakeholders, and any significant differences between the two regimes would create compliance complexities.

A detailed comparison reveals several important distinctions [10]:

- **Privacy Impact Assessments (PIAs):** Law 25 mandates the completion of PIAs for any project involving the processing of personal information and before transferring information outside of Quebec. The CPPA had no equivalent mandatory PIA requirement, though it did require a "legitimate interest assessment" for that specific consent

exception.

- **Automated Decision-Making:** Law 25's provisions apply to decisions based *exclusively* on automated processing and give individuals the right to submit observations for human review. The CPPA's right to an explanation applied more broadly to systems that could have a "significant impact" but did not include a right to human review.
- **Right to Erasure:** Quebec's law includes a "right to de-indexation," allowing an individual to compel an organization to stop disseminating their information or to de-link it from their name. This is a subtly different and potentially broader right than the CPPA's right to disposal.
- **Enforcement:** The most significant difference was in enforcement. Quebec's regulator, the Commission d'accès à l'information (CAI), has the power to directly impose administrative monetary penalties, mirroring the GDPR model and contrasting sharply with the OPC/PIDPTA structure proposed in Bill C-27.

The following table provides a clear, at-a-glance summary of how the CPPA's key provisions stacked up against these two critical legal frameworks.

Feature	**Bill C-27 (CPPA)**	**Quebec Law 25**	**EU GDPR**
Primary Basis for Processing	Consent (Express default). "Legitimate Interest" as an *exception* to consent.	Consent. Exceptions for new purposes with a direct, relevant connection.	Choice of 6 lawful bases, including Consent and "Legitimate Interests."
Key Individual Rights	Disposal (Erasure), Portability, Algorithmic Transparency.	De-indexation/Cease Dissemination, Portability, Algorithmic Transparency.	Erasure, Portability, Restriction of Processing, Objection, Automated Decision-Making rights.
Enforcement Model	OPC investigates and *recommends* penalties to a separate Tribunal (PIDPTA).	CAI (regulator) can *directly impose* penalties.	Data Protection Authorities (DPAs) can *directly impose* fines.
Maximum	Greater of $10M or	Greater of $10M or	Up to €20M or 4%

Administrative Penalty	3% of global revenue.	2% of global revenue.	of global annual turnover.
Maximum Offence Fine	Greater of $25M or 5% of global revenue.	Greater of $25M or 4% of global revenue.	N/A (Penalties are administrative).

This comparative analysis demonstrates that while Bill C-27 made significant strides toward modernization, it often stopped short of fully adopting the standards set by its key international and domestic counterparts, particularly in the crucial area of enforcement.

7. Conclusion: The Unfinished Legacy of Bill C-27 and the Path Forward

7.1 The Impact of the 2025 Prorogation

The legislative journey of Bill C-27 came to an abrupt end on January 6, 2025. The prorogation of Parliament, a constitutional procedure that concludes a session, resulted in all bills that had not received Royal Assent being "entirely terminated".[20] This included not only Bill C-27 but also other significant pieces of digital policy legislation, such as Bill C-26 (cybersecurity) and Bill C-63 (online harms).[16] While it is procedurally possible for a government to reintroduce a bill from a previous session, the political context at the time made such a move for C-27 in its original form highly unlikely.[23] The effect was to send the federal government's efforts on comprehensive privacy and AI reform back to the starting line, leaving the 25-year-old PIPEDA as the law of the land.

7.2 Enduring Principles and Contentious Issues Likely to Resurface

Despite its ultimate failure to become law, Bill C-27 has left an indelible mark on the Canadian digital policy landscape. The extensive debate it sparked has fundamentally shifted the national conversation and established a new baseline of expectations for any future reform.

The core principles advanced in the bill—the need for stronger and more meaningful consent, the introduction of new digital rights like portability and erasure, and the imperative for AI accountability—are now widely seen as inevitable components of any modern data protection framework.[47]

However, the bill's failure also means that the most contentious and unresolved issues will certainly resurface in any subsequent legislative attempt. Any future government will have to grapple with the same fundamental questions that Bill C-27 failed to definitively answer [16]:

- **The Legal Status of Privacy:** Will privacy be treated as a quasi-constitutional, fundamental right that takes precedence, or as a consumer interest to be balanced against commercial objectives?
- **The Enforcement Model:** Should the federal privacy regulator be empowered with direct order-making and fining authority, or should an oversight body like the PIDPTA be maintained?
- **The Scope of Consent Exceptions:** How can the law provide flexibility for legitimate business activities without creating loopholes that render the principle of consent meaningless?
- **The Approach to AI Regulation:** How can Canada craft effective, rights-respecting, and innovation-friendly legislation for AI, and should this be done within an omnibus privacy bill or as a standalone initiative?

7.3 Strategic Outlook for Canadian Digital Policy

In the immediate aftermath of Bill C-27's demise, the Canadian regulatory landscape remains fragmented. Quebec's Law 25 now stands as the most stringent privacy legislation in the country, creating a powerful incentive for businesses operating nationwide to adopt its higher standards as their default to ensure compliance.[22] This reality puts significant pressure on the federal government and other provinces to modernize their own laws to create a more harmonized national framework.

The experience with Bill C-27 offers a clear lesson for the path forward. The widespread and unified opposition to the inclusion of the *Artificial Intelligence and Data Act* strongly suggests that future attempts to regulate AI will need to be undertaken through a separate, standalone legislative process.[16] This would allow for the dedicated and in-depth consultation with experts, civil society, and industry that AIDA so clearly lacked.

The legacy of Bill C-27 is therefore a dual one. It is a story of legislative failure, but also one of profound, if incomplete, progress. The bill successfully brought the complex and often technical issues of data privacy and AI governance to the forefront of national debate. The

hundreds of hours of testimony and the dozens of detailed briefs submitted to the INDU committee now form an invaluable, if informal, public record. This body of evidence, forged in the crucible of parliamentary debate, will undoubtedly serve as the foundational text for the next, and necessary, attempt to write Canada's digital charter into law.

Works cited

1. Five things to know about Bill C-27 - Schwartz Reisman Institute - University of Toronto, accessed October 1, 2025, https://srinstitute.utoronto.ca/news/five-things-to-know-about-bill-c-27
2. Canada's Bill C-27: Modernizing Data Privacy Laws in 2024 - TRUENDO, accessed October 1, 2025, https://www.truendo.com/blog/canadas-bill-c-27-modernizing-data-privacy-laws-in-2024
3. Bill C-27 (Historical) - OpenParliament.ca, accessed October 1, 2025, https://openparliament.ca/bills/44-1/C-27/
4. Legislative Summary of 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 - Library of Parliament, accessed October 1, 2025, https://lop.parl.ca/sites/PublicWebsite/default/en_CA/ResearchPublications/LegislativeSummaries/441C27E
5. Canada's Digital Charter, accessed October 1, 2025, https://ised-isde.canada.ca/site/innovation-better-canada/en/canadas-digital-charter-trust-digital-world
6. Bill C-27 - House of Commons, accessed October 1, 2025, https://www.ourcommons.ca/Content/Committee/441/INDU/Brief/BR12448397/br-external/UNICEFCan-e.pdf
7. C-27 (44-1) - LEGISinfo - Parliament of Canada, accessed October 1, 2025, https://www.parl.ca/legisinfo/en/bill/44-1/c-27
8. Bill C-27 summary: Digital Charter Implementation Act, 2022, accessed October 1, 2025, https://ised-isde.canada.ca/site/innovation-better-canada/en/canadas-digital-charter/bill-summary-digital-charter-implementation-act-2020
9. Policy Detail - Bill C-27: Digital charter implementation act - OECD DPP, accessed October 1, 2025, https://depp.oecd.org/policies/CAN1238
10. An Evolving Digital Privacy Landscape—Comparing the Federal Bill ..., accessed October 1, 2025, https://www.mccarthy.ca/en/insights/blogs/techlex/evolving-digital-privacy-landscape-comparing-federal-bill-c-27s-cppa-quebecs-bill-64
11. 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 - Department of Justice Canada, accessed October 1, 2025, https://www.justice.gc.ca/eng/csj-sjc/pl/charter-charte/c27_1.html

12. Bill C-27 - Gowling WLG, accessed October 1, 2025, https://gowlingwlg.com/en-ca/topics/canadian-privacy-laws-new-rules-for-a-new-era/bill-c-27
13. 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, accessed October 1, 2025, https://www.ourcommons.ca/Content/Committee/441/INDU/Brief/BR12942185/br-external/ImagineCanada-e.pdf
14. Digital Charter Implementation Act - IAB Canada, accessed October 1, 2025, https://iabcanada.com/iab-standards-and-guidelines/digital-charter-implementation-act/
15. Bill C-27: The Digital Charter Implementation Act Proposed Legislation to Modernize Canadian Privacy Law - Sherrard Kuzz LLP, accessed October 1, 2025, https://www.sherrardkuzz.com/wp-content/uploads/2024/08/Briefing-Note-Bill-C-27-The-Digital-Charter-Implementation-Act-August-6-2024-Final.pdf
16. Privacy and cyber bills What to expect post election - Gowling WLG, accessed October 1, 2025, https://gowlingwlg.com/en-fr/insights-resources/articles/2025/privacy-and-cyber-bills-what-to-expect-post-election
17. Consumer Privacy Protection Act (Canada's Bill C-27): Feedback from industry participants, accessed October 1, 2025, https://www.blg.com/en/insights/2023/01/consumer-privacy-protection-act-canadas-bill-c-27-feedback-from-industry-participants
18. Balancing Stakeholder Interests in Bill C-27 - Centre for International Governance Innovation (CIGI), accessed October 1, 2025, https://www.cigionline.org/publications/balancing-stakeholder-interests-in-bill-c-27/
19. Canadian businesses concerned AI bill moving forward without their testimony - National, accessed October 1, 2025, https://globalnews.ca/news/10341415/ai-bill-c-27-canada/
20. Canada: Bill C-27 dies after Parliament is prorogued | News ..., accessed October 1, 2025, https://www.dataguidance.com/news/canada-bill-c-27-dies-after-parliament-prorogued
21. What's Next After AIDA? - Schwartz Reisman Institute - University of Toronto, accessed October 1, 2025, https://srinstitute.utoronto.ca/news/whats-next-for-aida
22. Looking ahead: the Canadian privacy and AI landscape without Bill C-27 - Torys LLP, accessed October 1, 2025, https://www.torys.com/our-latest-thinking/publications/2025/01/the-canadian-privacy-and-ai-landscape-without-bill-c-27
23. Prorogation's Digital Impact: Canada's Digital Bills Set to Die on the Order Paper - Fasken, accessed October 1, 2025, https://www.fasken.com/en/knowledge/2025/01/prorogations-digital-impact
24. Canada's new federal privacy Bill C-27 – Summary of significant impacts and new

proposals, accessed October 1, 2025, https://www.dentons.com/en/insights/articles/2022/june/20/canadas-new-federal-privacy-bill-c27-summary-of-significant-impacts-and-new-proposals
25. Issue Sheets on the Study of Bill C-27 - Office of the Privacy Commissioner of Canada, accessed October 1, 2025, https://www.priv.gc.ca/en/privacy-and-transparency-at-the-opc/proactive-disclosure/opc-parl-bp/indu_20231019/is_c27_20231019/
26. Bill C-27, Digital Charter Implementation Act, 2022, accessed October 1, 2025, https://www.ourcommons.ca/Content/Committee/441/INDU/Brief/BR12950092/br-external/CanadianBarAssociationPrivacyAndAccessLawSection-2022-e.pdf
27. Submission on Bill C-27: An Act to enact the Consumer Privacy Protection Act, the Personal Information and Data Protection Tribu, accessed October 1, 2025, https://www.ourcommons.ca/Content/Committee/441/INDU/Brief/BR12631608/br-external/CanadianLifeAndHealthInsuranceAssociation-e.pdf
28. Submission to the Standing Committee on Industry and Technology ..., accessed October 1, 2025, https://chamber.ca/submission-to-the-standing-committee-on-industry-and-technology-on-bill-c-27/
29. Submission on Bill C-27, Digital Charter Implementation Act to House of Commons Standing Committee on Industry and Technology , October 26, 2023. - Colin Bennett, accessed October 1, 2025, https://www.colinbennett.ca/blog/submission-on-bill-c-27-digital-charter-implementation-act-to-house-of-commons-standing-committee-on-industry-and-technology-october-26-2023/
30. An update of C-27 since its reintroduction in Parliament - IAPP, accessed October 1, 2025, https://iapp.org/news/a/an-update-of-c-27-since-its-reintroduction-in-parliament
31. Appearance before the Standing Committee on Industry and Technology (INDU) by the Minister of Innovation, Science, and Industry - Transparency, accessed October 1, 2025, https://ised-isde.canada.ca/site/transparency/en/appearance-standing-committee-industry-and-technology-indu-minister-innovation-science-and-industry-0
32. Bill C-27 (Historical) - OpenParliament.ca, accessed October 1, 2025, https://openparliament.ca/bills/44-1/C-27/?tab=mentions
33. Proposed Changes to Canada's Bill C-27 Do Little to Mitigate AI Harms, accessed October 1, 2025, https://www.cigionline.org/articles/proposed-changes-to-canadas-bill-c-27-do-little-to-mitigate-ai-harms/
34. Canadian Parliament's Bill C-27 hearing delves deeper into AIDA | IAPP, accessed October 1, 2025, https://iapp.org/news/a/canadian-parliaments-bill-c-27-hearing-delves-deeper-into-aida
35. 1 House of Commons Canada Standing Committee on Industry and Technology (INDU) Brief on Bill C-27 An Act to enact the Consumer P, accessed October 1,

2025, https://www.ourcommons.ca/Content/Committee/441/INDU/Brief/BR12819643/br-external/Jointly9-10815945-e.pdf
36. Bill C-27: Upcoming amendments to privacy and AI legislation - BLG, accessed October 1, 2025, https://www.blg.com/en/insights/2023/10/bill-c-27-upcoming-amendments-to-privacy-and-ai-legislation
37. Bill C-27: Federal Government Releases Amendments to Canada's ..., accessed October 1, 2025, https://www.fasken.com/en/knowledge/2023/12/bill-c27-federal-government-releases-amendments-to-canadas-proposed-ai-law
38. Submissions to the House of Commons Standing Committee on Industry and Technology regarding Bill C-27, An Act to enact the Consumer Privacy Protection, accessed October 1, 2025, https://www.ourcommons.ca/Content/Committee/441/INDU/Brief/BR12951872/br-external/BritishColumbiaCivilLibertiesAssociation-e.pdf
39. Brief on Bill C-27: An Act to enact the Consumer Privacy - House of Commons, accessed October 1, 2025, https://www.ourcommons.ca/Content/Committee/441/INDU/Brief/BR12598706/br-external/InternationalCivilLibertiesMonitoringGroup-e.pdf
40. Canada Bill C-27 (AIDA) - Proposed Amendments February 2024 ..., accessed October 1, 2025, https://www.ourcommons.ca/Content/Committee/441/INDU/Brief/BR12948163/br-external/MetaPlatformsInc-e.pdf
41. 1 Submissions on Bill C-27 The Digital Charter Implementation Act Submitted by Jane Bailey,1 Jacquelyn Burkell,2 and Brenda McPh, accessed October 1, 2025, https://www.ourcommons.ca/Content/Committee/441/INDU/Brief/BR12605252/br-external/Jointly3-e.pdf
42. News | CIPPIC, accessed October 1, 2025, https://www.cippic.ca/our-work/latestnews
43. Prepared by - House of Commons, accessed October 1, 2025, https://www.ourcommons.ca/Content/Committee/441/INDU/Brief/BR12793483/br-external/Jointly8-e.pdf
44. Recommendations on Canada's first legislation addressing artificial intelligence. - CAPE, accessed October 1, 2025, https://www.acep-cape.ca/sites/default/files/2024-01/Submission%20to%20INDU_Bill%20C%2027_AI.pdf
45. Canada: An overview of Bill C-27 and its proposed changes to ..., accessed October 1, 2025, https://www.dataguidance.com/opinion/canada-overview-bill-c-27-and-its-proposed-changes
46. Proposed Canadian Privacy Bill Introduces Fines and New Requirements for Private Organizations, accessed October 1, 2025, https://www.americanbar.org/groups/business_law/resources/business-law-today/2022-july/proposed-canadian-privacy-bill/

47. Bill C-27: The Future of Canadian Privacy Law - Cookie Script, accessed October 1, 2025, https://cookie-script.com/privacy-laws/bill-c27