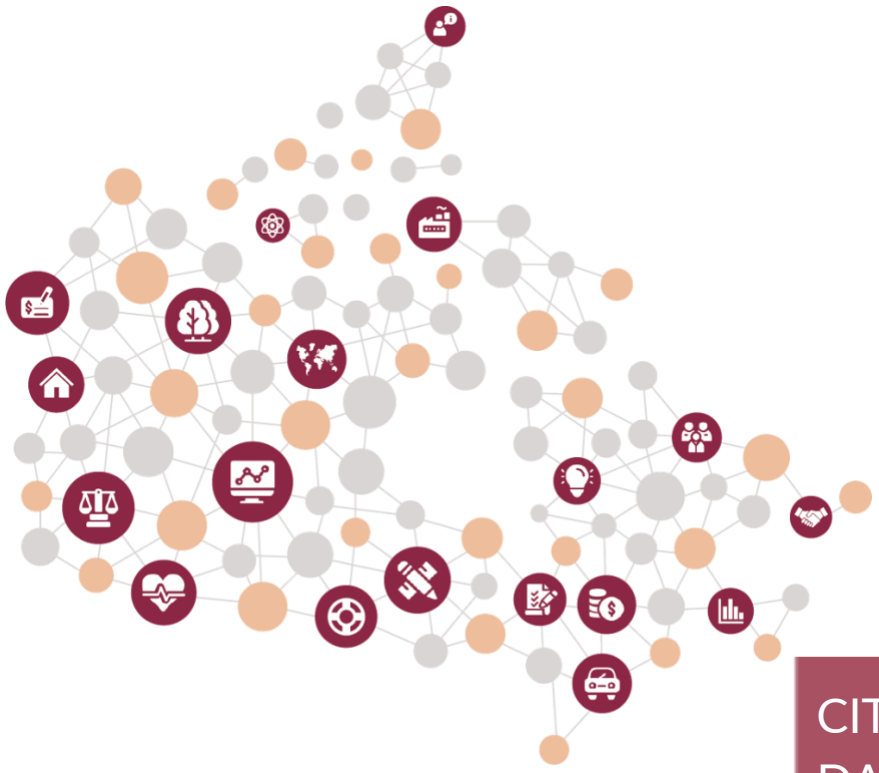
CIRANO

Knowledge into action



CITIZEN-CENTRIC PUBLIC SECTOR DATA INTEROPERABILITY IN CANADA: ENABLING A MUTUALIZED SOVEREIGN CAPACITY

ALAIN DUDOIT
ANNE-MARIE HUBERT
TONY LABILLOIS

PR 2026PR-07
FOR REFLECTION

CIRANO
Knowledge into action

Les documents **Pour Réflexion** sont des documents publiés pour susciter échanges et commentaires et s'appuient sur des résultats de recherche. Ces documents sont sous la seule responsabilité des auteurs.

Reflection Papers are documents published to stimulate discussion and commentary, based on research findings. These documents are the sole responsibility of their authors.

Le CIRANO est un organisme sans but lucratif constitué en vertu de la Loi des compagnies du Québec. Le financement de son infrastructure et de ses activités de recherche provient des cotisations de ses organisations-membres, d'une subvention d'infrastructure du gouvernement du Québec, de même que des subventions et mandats obtenus par ses équipes de recherche.

CIRANO is a private non-profit organization incorporated under the Quebec Companies Act. Its infrastructure and research activities are funded through fees paid by member organizations, an infrastructure grant from the government of Quebec, and grants and research mandates obtained by its research teams.

Les partenaires du CIRANO – *CIRANO Partners*

Partenaires Corporatifs - Corporate Partners	**Partenaires gouvernementaux - Governmental partners**	**Partenaires universitaires - University Partners**
Autorité des marchés financiers	Ministère des Finances du Québec	École de technologie supérieure
Banque de développement du Canada	Ministère de l'Économie, de l'Innovation et de l'Énergie	École nationale d'administration publique
Banque du Canada	Innovation, Sciences et Développement Économique Canada	HEC Montréal
Banque Nationale du Canada	Ville de Montréal	Institut national de la recherche scientifique
Bell Canada		Polytechnique Montréal
BMO Groupe financier		Université Concordia
La Caisse		Université de Montréal
Énergir		Université de Sherbrooke
Hydro-Québec		Université du Québec
Intact Corporation Financière		Université du Québec à Montréal
Mouvement Desjardins		Université Laval
Power Corporation du Canada		Université McGill
Pratt & Whitney Canada		
VIA Rail Canada		

Le CIRANO collabore avec de nombreux centres et chaires de recherche universitaires dont on peut consulter la liste sur son site web. *CIRANO collaborates with many centers and university research chairs; list available on its website.*

Les idées et les opinions émises dans cette publication sont sous l'unique responsabilité des auteurs et ne représentent pas les positions du CIRANO ou de ses partenaires. *The observations and viewpoints expressed in this publication are the sole responsibility of the authors; they do not represent the positions of CIRANO or its partners.*

ISSN 2563-7266 (version en ligne)

Citizen-Centric Public Sector Data Interoperability in Canada: Enabling a Mutualized Sovereign Capacity

Alain Dudoit
Ambassador of Canada (ret.)
CIRANO Invited Fellow
Strategic Advisor, Global Advantage Consulting Group

Anne-Marie Hubert
CIRANO Invited Fellow
Special Advisor to the IFRS Foundation
Former member of the Global Advisory Council of EY and of EY Canada's Executive Committee

Tony Labillois
Consultant in accessibility, public policy, leadership, and data
Retired Director General at Statistics Canada
Elected Member of the International Statistical Institute

May 11, 2026

Pour citer ce document / To quote this document

Dudoit, A., Labillois, T & Hubert, A-M (2026). Citizen-Centric Public Sector Data Interoperability in Canada: Enabling a Mutualized Sovereign Capacity (2026PR-07, Fore Reflection, CIRANO). https://doi.org/10.54932/LQEY7039

Table of contents

Summary/Abstract

French

Cet article soutient que le Canada se trouve à un point de bascule dans l'évolution de sa gouvernance numérique : les conditions sont désormais réunies pour passer d'une coopération intergouvernementale sectorielle à une capacité d'action coordonnée fondée sur l'interopérabilité des données publiques et l'adoption responsable de l'intelligence artificielle (IA).

S'appuyant sur le précédent structurant de l'accord fédéral–provincial–territorial (FPT) sur la cybersécurité conclu à Kananaskis en 2025, l'analyse montre que la protection des systèmes ne constitue qu'une première étape. La pleine valeur des investissements numériques dépend de la capacité des gouvernements à permettre une circulation sécurisée, gouvernée et ciblée des données entre juridictions. Dans ce contexte, l'interopérabilité n'apparaît pas comme un enjeu technique, mais comme une infrastructure stratégique conditionnant la performance économique, la qualité des services publics et la capacité d'anticipation du secteur public.

L'article met en évidence une contrainte structurelle : malgré l'existence de stratégies ambitieuses et de cas d'usage concrets en matière d'IA, la fragmentation des systèmes de données limite les gains potentiels et empêche l'émergence d'effets systémiques. Cette fragmentation constitue moins un déficit technologique qu'un déficit d'architecture institutionnelle et de mécanismes de confiance à l'échelle FPT.
À partir d'une analyse comparative d'expériences internationales, notamment en Europe et en Australie, l'article démontre la faisabilité d'un modèle fédéré reposant sur des normes communes, des mécanismes de gouvernance partagée et une mutualisation ciblée des capacités, sans centralisation des données.

Sur cette base, il propose un prototype d'accord-cadre FPT conçu comme une base opérationnelle de concertation intergouvernementale. Cet avant-projet articule des principes structurants, une architecture de gouvernance, des instruments techniques et juridiques, ainsi que des mécanismes de mise en œuvre progressive. Il vise à concilier autonomie des juridictions et capacité d'action collective, en introduisant des dispositifs tels que l'évaluation de l'interopérabilité, les bacs à sable et des accords sectoriels d'échange de données encadrés.
L'article conclut que le Canada ne fait pas face à un déficit de diagnostic, mais à un impératif de mise en cohérence. Dans un environnement international marqué par la montée des dépendances technologiques et la centralité des données, la capacité à organiser ces dernières comme une architecture fédérée interopérable devient un déterminant stratégique de souveraineté, de résilience et de prospérité.

English

This paper argues that Canada has reached a tipping point in the evolution of its digital governance: the conditions are now in place to move from sectoral intergovernmental cooperation towards a coordinated capacity for action based on public data interoperability and the responsible adoption of artificial intelligence (AI).

Building on the precedent set by the 2025 federal-provincial-territorial (FPT) cybersecurity agreement concluded in Kananaskis, the analysis shows that securing systems is only the first step. The full value of digital investments now depends on governments' ability to enable the secure, governed, and targeted circulation of data across jurisdictions. In this context, interoperability should not be viewed as a technical issue, but as a strategic infrastructure that shapes economic performance, public service delivery, and the public sector's capacity to anticipate and act.

The paper identifies a structural constraint: despite ambitious strategies and concrete AI use cases, the fragmentation of public data systems limits potential gains and prevents the emergence of system-wide effects. This fragmentation reflects not a technological deficit, but an institutional and governance gap, particularly in terms of trust mechanisms at the FPT level. Drawing on international experience, particularly from the European Union and Australia, the paper demonstrates the feasibility of a federated model based on shared standards, joint governance mechanisms, and targeted mutualization of capabilities, without centralizing data.

On this basis, it introduces a prototype FPT framework agreement designed as an operational foundation for intergovernmental negotiation. The proposal combines guiding principles, governance architecture, technical and legal instruments, and a phased implementation approach. It seeks to reconcile jurisdictional autonomy with collective capacity, notably through mechanisms such as interoperability assessments, regulatory sandboxes, and structured sectoral data-sharing agreements.

The paper concludes that Canada does not face a diagnostic gap, but a coordination imperative. In a global environment shaped by technological dependencies and the growing centrality of data, the ability to organize public data as a federated interoperable architecture is becoming a key determinant of sovereignty, resilience, and long-term prosperity.

Introduction: A window of opportunity not to be missed

Canada no longer faces a lack of vision regarding artificial intelligence, but a lack of integration of its own public capabilities.

The federal-provincial-territorial meeting in Kananaskis in 2025, marked by the conclusion of an agreement on cybersecurity, set a defining precedent: that of governments' ability to act collectively in the face of digital challenges now recognized as strategic. Since then, political, technological, and institutional conditions have evolved significantly, to the point where a further step is now possible: the transition from sectoral cooperation to a federated architecture.

This evolution is no longer based on assumptions, but on recent converging developments. The Government of Canada has just published the Spring 2026 Economic Update in which it sets out its vision of artificial intelligence for all; this proposed strategy *"**will help** accelerate the adoption of AI by small and medium-sized enterprises **and transform the delivery of public services to better serve Canadians**.* At the same time, the overview of artificial intelligence applications published by the Government of Quebec shows that these technologies are already being deployed in practice within public administratio**ns**, with a variety of use cases and a genuine capacity for innovation.

Taken together, these developments reveal a clear trend: Canada now has a strategic vision for artificial intelligence and a tangible basis for administrative experimentation. What is lacking, however, is neither the vision nor the capacity for innovation, but the architecture to ensure their coherence. In the absence of effective interoperability of public data at the federal, provincial, and territorial levels, these initiatives risk remaining fragmented, limiting their systemic impact.
It is precisely in this gap, between strategic ambition and integration capacity, that the current window of opportunity lies. The conditions necessary for a coordinated transformation are now in place: political recognition of the issues, emerging technical capabilities, and an institutional precedent demonstrating the feasibility of collective action. In this context, the question is no longer whether to act, but how to structure that action.

This article seeks to answer that question by building on the spirit of Kananaskis. It argues that the next step is not to multiply initiatives, but to link them together. To this end, it proposes a draft framework agreement between the federal, provincial, and territorial governments on the interoperability of public data and the adoption of artificial intelligence, not as a conceptual exercise, but as an operational basis for negotiation.

In an environment marked by geopolitical fragmentation, the rise of technological dependencies and the growing centrality of data to states' capacity for action, the ability to organize this data as a coherent system is becoming a strategic determinant. The issue is no longer merely administrative or technological: it is now institutional, economic and, increasingly, linked to sovereignty.

From this perspective, the proposed framework agreement is not just one option among many. It appears to be the instrument capable of transforming what is still only partial convergence into an integrated capacity for action across Canada.

The federal government is preparing to launch a structured strategy on artificial intelligence; public administrations, particularly in Quebec, are already demonstrating its practical applications. What is lacking is neither vision nor capacity, but the architecture needed to ensure consistency. Without data interoperability at the federal-provincial-territorial level, these initiatives will remain fragmented. The proposed framework agreement is specifically designed to address this structural shortcoming. The proposed approach is explicitly rooted in a spirit of collaborative federalism, where interoperability aims to strengthen the capacity for action of jurisdictions without altering their powers or reducing their decision-making autonomy.

At this stage, the objective is not so much to draw up a new strategic statement, but rather to foster the emergence of a collaborative organizational structure capable of sustainably supporting data interoperability, the informed integration of artificial intelligence and the continuous improvement of public service delivery. The analytical, institutional, and political conditions necessary for this transition now appear to be largely in place. What remains is to clarify the implementation arrangements in order to ensure feasibility and buy-in.

Section 1 From cybersecurity to interoperability: broadening the scope of FPT cooperation

1.1 A turning point: the Kananaskis agreement as a landmark precedent

The signing of the federal-provincial-territorial (FPT) agreement on cybersecurity in October 2025, during the Kananaskis ministerial meeting, marks a major turning point in the recent evolution of intergovernmental cooperation in Canada. This agreement marks an explicit recognition of the systemic nature of digital risks and the need for a coordinated response across the entire public sector.

Beyond its immediate scope, this agreement sets a key institutional precedent: that of the FPT governments' ability to reach agreement on critical technological issues affecting national security, infrastructure resilience, and the continuity of public services simultaneously. It thus establishes a common foundation: a "shared defensive perimeter," from which a move towards a more integrated capability becomes not only possible, but logical and desirable.

1.2 A consolidation process still incomplete

In the months following this agreement, several developments have consolidated its scope and revealed its operational implications. Mechanisms for collaboration between Chief Information Officers (CIOs), the establishment of the Office of Digital Transformation, and initiatives regarding digital infrastructure have helped to strengthen an intergovernmental dynamic that already existed but had previously been fragmented. These advances remain partial, but they demonstrate a genuine capacity on the part of governments to align their approaches around common objectives when the political and strategic framework is clearly established.

1.3 The shifting focus: from security to data flow

At the same time, the acceleration of work on artificial intelligence, particularly in the context of the evolving Canadian legislative framework on data and AI, has highlighted the growing importance of the secure flow of data between jurisdictions. Similarly, the economic and social priorities identified in recent public policies, whether concerning productivity, housing, labour mobility, or infrastructure management, are increasingly and explicitly based on the ability to mobilize interoperable data at a system-wide level.

1.4 From protection to activation: a shift in public policy

These converging developments are helping to shift the focus of interoperability from the technical register to the capacity for collective action. They bring into sharper relief a reality that already exists: the systems are in place, the data exists, and investments are underway, but their full value remains dependent on their ability to be mobilized in a coordinated manner across jurisdictions. This shift is based on a fundamental distinction. Cybersecurity aims to protect systems. Data interoperability aims to unlock their potential.

But, beyond this functional distinction, the real challenge is economic, social, and human in nature. The protection of systems contributes to the security of institutions. The activation of data, for its part, determines the ability of governments to tangibly improve citizens' lives by enhancing the quality and continuity of public services, supporting economic prosperity, facilitating mobility, and ensuring the effective exercise of rights in an integrated digital environment. Thus, cybersecurity protects the integrity of systems. Interoperability enables this potential to be translated into public value. In other words, security is a necessary but not sufficient condition for the capacity for public action in a digital environment. A perfectly secure but siloed system remains structurally limited in its ability to generate collective value, support decision-making and respond effectively to cross-cutting challenges.

1.5 The systemic effects of non-interoperability

This limitation is particularly evident in data-intensive sectors such as healthcare, emergency response, critical infrastructure, and labour mobility, where performance depends directly on the ability to share, access, cross-reference and utilize information across jurisdictions. In these contexts, the lack of interoperability creates invisible yet decisive friction: delays in decision-making, duplication of effort, operational inconsistencies, and a loss of value in existing data.

From this perspective, data interoperability can be understood as the functional extension of cybersecurity. It is not a separate initiative, but the realization of the potential of now-secure infrastructures. This framing allows the issue to be repositioned not as a new burden for governments, but as the logical continuation of a commitment already made.

1.6 Interoperability as strategic infrastructure

This shift from protection to activation also corresponds to a broader transformation of the role of data in public policy. Data can no longer be viewed solely as administrative resources, but as components of a strategic infrastructure, on a par with energy or transport networks. In this context, its ability to circulate efficiently, securely and in a controlled manner becomes a direct determinant of the system's overall performance.

1.7 The amplifying role of artificial intelligence

Artificial intelligence (AI) further accentuates this dynamic. As an infrastructure for processing and leveraging data, it depends directly on the quality, accessibility, and compatibility of that data. Without interoperability, AI applications remain confined to limited scopes, restricting their impact and their ability to generate systemic gains. Conversely, an environment of interoperable data enables the development of cross-cutting applications with significant leverage, particularly in the areas of planning, risk management, and the optimization of public services.

Consequently, the combination of cybersecurity and interoperability does not represent a series of separate initiatives, but rather a unified path towards an integrated public capacity. Cybersecurity ensures trust, interoperability enables data flow, and AI generates value.

1.8 Towards a collaborative operational federalism

In this context, broadening the scope of FPT cooperation to include data interoperability appears to be a natural evolution, building on recent achievements and consistent with the principles of Canadian federalism. This is not a matter of calling into question the autonomy of jurisdictions, but of creating the conditions for their effective collaboration around common objectives. This approach is part of a framework of operational federalism, where cooperation is not based on the centralization of systems, but on their ability to interact according to shared rules. It is based on targeted, consensual pooling of resources, standards, interfaces, and trust mechanisms, rather than on institutional integration.

In this sense, interoperability should not be viewed as a technical project, but as a strategic infrastructure for practical collaboration. It constitutes the mechanism through which the existing capabilities of different jurisdictions can be mobilized in a coherent, effective, and timely manner to address common challenges.

1.9 A political issue

Recent experience with cybersecurity demonstrates that this type of collaboration is possible. It also suggests that the political and institutional conditions necessary for such a development are now in place. The challenge is, therefore, no longer to establish the relevance of this approach, but to define the terms of its implementation and its sustainability. The issue is therefore no longer merely technical or administrative.
It becomes explicitly political: how to organize, at the system level, the conditions enabling governments to act in a coherent, secure, and effective manner within a federated digital environment.

Section 2, Why an FPT framework agreement is not only possible, but necessary

2.1 A transformation that goes beyond administrative modernization

The digital transformation of the public sector in Canada can no longer be viewed as a juxtaposition of sectoral initiatives or administrative modernization. It now takes place within an environment characterized by the acceleration of artificial intelligence, the rise of technological dependencies and the growing centrality of data to governments' capacity for action. In this context, the current fragmentation of public data systems across jurisdictions, sectors and institutions is no longer merely a matter of organizational inefficiency. It is becoming a limiting factor in economic performance, the quality of public services and, increasingly, the state's ability to anticipate and act in a coherent manner.

2.2 A disconnect between strategic vision and implementation

Recent developments provide empirical confirmation of the assessment set out in the introduction. The Spring 2026 Government of Canada's Economic Update formalizes a structured vision of artificial intelligence as a lever for economic, institutional, and democratic transformation. In particular, it emphasizes trust, large-scale adoption, infrastructure sovereignty, and the development of international alliances.
At the same time, the overview of how artificial intelligence is used in Quebec's public administration provides a practical insight into this transformation, documenting a range of use cases already implemented within public bodies.
This combination speaks volumes. It shows that Canada is neither at the early stage of merely defining strategies, nor at the later stage of fully coherent implementation, but in an intermediate phase characterized by a disconnect between vision and execution.

It is precisely this disconnect that constitutes the structural problem addressed in this article. In the absence of effective interoperability of public data at the federal, provincial, and territorial levels, these initiatives remain fragmented and cannot produce the expected systemic effects. While these initiatives have enabled real progress, they do not allow for the creation of a distributed capacity across the FPT system.

2.3 Fragmentation as a structural problem

Current approaches still rely heavily on compartmentalized sectoral, institutional, or technological approaches. This situation has several structural consequences. Firstly, information fragmentation, which limits visibility into economic, social, and territorial dynamics and complicates collaboration on public interventions. Secondly, a duplication of efforts and investments, with each jurisdiction developing its own solutions, which are often incompatible with one another, thereby reducing potential efficiency gains.

The current fragmentation does not eliminate risks; it simply makes them less visible and more difficult to manage. Compartmentalized, uncoordinated systems based on heterogeneous architectures already create significant vulnerabilities: inconsistencies in decision-making, information blind spots, implicit dependencies, and an inability to anticipate systemic effects. The analysis of risks associated with the use of artificial intelligence in public services (Tusikov N., Haggart B.) highlights real and well-documented challenges. Recent cases, both in Canada and internationally, demonstrate that poorly designed automated systems can produce significant errors and, in some cases, serious human consequences. However, these examples call for a more systemic interpretation. The failures observed do not stem primarily from artificial intelligence as such, but from the conditions under which it is deployed. They reveal not so much a uniform approach to system integration as a persistent fragmentation of data, processes, and governance mechanisms.

In an environment where data is siloed, standards are heterogeneous and validation mechanisms are limited, AI acts as an amplifier of existing inconsistencies. Conversely, in an ecosystem based on interoperability, common rules, and trust mechanisms, it can become a tool for consistency, error detection, and continuous improvement. The central question is therefore not whether to slow down the adoption of AI in public services, but to determine within which institutional and informational architecture it is deployed.

2.4 The threshold effect associated with artificial intelligence

This dynamic creates a threshold effect. Below a certain level of data integration, the benefits associated with AI remain marginal. Above this threshold, they become exponential. The current fragmentation prevents the Canadian public sector from crossing this threshold at a system-wide level. Furthermore, this dynamic rapidly reduces the room for manoeuvre of public systems that fail to link their data on the required scale, creating a growing gap between potential capabilities and those actually utilized.

2.5 The practical impacts on citizens

These limitations have direct repercussions for citizens. They manifest themselves in fragmented administrative processes, discontinuous public services, and delays in accessing essential benefits or interventions. In areas such as health, employment or social services, the lack of interoperability can lead to information gaps that affect the quality of services, the speed of interventions and, ultimately, the quality of life of those concerned. Conversely, improved data flow would enable the provision of smoother services that are better tailored to citizens' needs and more consistent across jurisdictions. The accelerating pace of AI-related transformations is placing additional pressure on existing systems. AI relies on access to vast, diverse, and high-quality datasets. It widens the gap between organizations capable of harnessing this data and those that remain confined to information silos. However, this structural dependence on data cannot be separated from other conditions that are equally crucial for sustainable implementation.

Beyond infrastructure and access to data, the public sector's ability to take full advantage of artificial intelligence also depends on the availability of talent and on maintaining a high level of trust in how it is deployed. This aspect is fundamental. It determines not only the quality of the solutions developed, but also their social and institutional acceptability.
From this perspective, skill development, support for professional transitions and the integration of clear principles regarding the responsible use of AI appear to be complementary levers to data interoperability. They help to anchor this transformation on a trajectory that is both effective and sustainable, ensuring that the benefits associated with AI are part of a framework of shared value creation and lasting trust.

2.6 A shortfall in architecture, not in capacity

Greater exposure to external technological dependencies, insofar as the lack of critical mass and collaboration, limits the ability to develop and operate infrastructure and systems at the federal level; these limitations do not stem from a lack of capacity or innovation, but from a lack of architectural framework. They reflect the absence of a framework to link existing initiatives in a coherent manner for the benefit of citizens.
Previous work has also highlighted that the main barriers to interoperability are not technological, but institutional and political. The required technologies, such as open standards, secure APIs and cloud architectures, are readily available and well understood.

What is lacking is a framework to enable their coordinated adoption at the intergovernmental level. Interoperability relies less on technological choices than on trust mechanisms: shared standards, common rules, and appropriate compliance and governance mechanisms. This aspect is particularly relevant in the Canadian context, where the diversity of jurisdictions requires solutions compatible with a high degree of institutional autonomy.

The establishment of a federated framework for public data interoperability appears not as a secondary condition, but as a prerequisite for the responsible and effective use of artificial intelligence. Without such an architecture, the identified risks are likely to multiply. With it, they can be structured, managed, and gradually reduced.

2.7 Growing international pressure

Furthermore, the ongoing transformations in the international environment are reinforcing this pressure. The rise of large-scale interoperability models, particularly in Europe, demonstrates that it is possible to reconcile federated governance, respect for jurisdictions and system integration. These experiences help to overcome some of the political objections traditionally associated with this type of approach.
In the absence of a common structural framework, each initiative must define its own rules, standards, and governance mechanisms. This situation leads to a proliferation of mutually incompatible solutions, paradoxically reinforcing the very fragmentation they seek to reduce.

2.8 A genuine window of opportunity

While the need for collaborative FPT action is now clear, its feasibility depends on several converging factors. Politically, the precedent set by cooperation on cybersecurity demonstrates that collective action is possible when the issues are recognized as strategic. Technologically, the growing maturity of standards, cloud architectures and interoperability tools makes technically feasible what was not possible just a few years ago. Institutionally, the proliferation of initiatives at federal and provincial levels can serve as a foundation upon which to build a federated architecture.

2.9 The framework agreement as a prerequisite for coherence

In this context, the establishment of a federal–provincial–territorial framework agreement appears not as an extension of existing policies, but as a prerequisite for their coherence and effective implementation. It would enable the transformation of a collection of initiatives into a structured capacity capable of producing system-wide effects.

2.10 Interoperability: controlled risk management

Mark Carney's speech in Davos served as a strategic revelation. He did not merely describe a global economic transformation but highlighted a fundamental constraint on contemporary public action: the growing inability of states to manage systemic risks without enhanced coordination, common standards, and effective access to actionable data.

His approach is based on a clear sequence: recognizing risks, acting coherently, establishing common frameworks, and reducing structural vulnerabilities. This logic extends beyond financial markets or the climate. It applies directly to public data governance. In his work on climate risks, Carney emphasizes a fundamental principle: without accessible, comparable, and reliable data, it is impossible to anticipate shocks, guide decisions and ensure an orderly transition. This idea resonates directly with the Canadian context.

Current challenges, whether economic, social, or environmental, share a common characteristic: they require coordinated decisions based on data distributed across jurisdictions.

However, in Canada, whilst this data exists, its fragmentation limits its use at a system-wide level. The challenge is, therefore, not the production of information, but its integration under secure, governed, and interoperable conditions. From this perspective, the interoperability of public data can be understood as an infrastructure for collective risk management. It enables the transformation of scattered information into a shared capacity for anticipation, supports the coherence of public interventions and reduces information asymmetries between jurisdictions. Thus, Prime Minister Carney's call for common standards, coordination mechanisms, and institutions capable of steering collective action finds concrete expression in the FPT context: the establishment of a structured framework for data interoperability.

Without such an architecture, strategic ambitions regarding artificial intelligence, economic transition or systemic resilience risk remain limited by a fundamental constraint: the inability to organize data as a collective asset that can be mobilized at the national level.

2.11 A strategic necessity, not an option

The question, therefore, is no longer whether better collaboration on public data is desirable, but whether Canada can afford not to achieve it. In an environment where the ability to understand, anticipate and act increasingly depends on the quality and quantity of evidence, FPT interoperability appears to be a fundamental prerequisite for public action. It constitutes the missing link between now-established strategies and their translation into concrete results. It is from this perspective that the following section examines international experiences, in order to shed light on the practical ways in which such an architecture can be designed and implemented in a federal context.

The challenge is not to choose between integration and caution, but to design an interoperability architecture capable of explicitly integrating the management of these risks. This requires a shift from an accumulation of systems to a governance model that is mindful of their interactions. It is precisely in this light that the establishment of an FPT framework agreement takes on its full significance. Far from accelerating uncontrolled dynamics, it would, on the contrary, make the interdependencies between systems explicit; provide a framework for the exchange and use of data; and structure a collective capacity for risk anticipation and management.

This gradual approach also appears relevant in contexts characterized by significant institutional diversity, particularly regarding relations with First Nations, where approaches based on experimentation and co-construction could serve as a key lever.

The conditions necessary for this exploration now appear to be in place: analytical convergence, institutional precedent in cybersecurity, technological maturity and growing pressure related to AI. This convergence creates a rare window of opportunity, in which the development of a structuring instrument becomes not only necessary, but possible. This development is part of a trend already observable at the international level, where several jurisdictions have undertaken to structure data interoperability within federated frameworks based on trust, standards, and shared governance.

Section 3 , What international experience shows: a federated model based on trust and standards

3.1 A demonstration of feasibility, not a model to be replicated

The international experience should not be viewed here as a model to be replicated, but as a demonstration of feasibility. It shows that it is possible to build a governance framework for interoperability that respects the autonomy of jurisdictions whilst enabling the secure flow of data, the reuse of solutions and the development of shared capabilities. In this regard, the experiences of the European Union and Australia are particularly instructive, not because they are identical to the Canadian case, but because they confirm that a federated framework can be flexible, robust, and politically acceptable. This interpretation is consistent with CIRANO's previous work, which has already presented interoperability as a strategic infrastructure, rather than a mere technical adjustment.

3.2 The case of the European Union: structured governance without centralization

In the European Union, the adoption of the Interoperable Europe Act has institutionalized enhanced cooperation on public sector interoperability at a cross-border level. The Interoperable Europe portal presents this initiative as a strategic cooperation mechanism for the entire Union, whilst the Interoperable Europe Board brings together high-level representatives from Member States and the European Commission to coordinate the interoperability of public services across national borders. The European framework thus establishes shared governance, without excessive centralization, but with a clear capacity for guidance, monitoring, and strategic alignment. The Regulation has been in force since 11 April 2024, making it a recent and concrete reference point for any discussion on data governance in a federated context.

3.3 An operational approach based on reuse

What is particularly relevant for Canada is not only the existence of a European framework, but the way in which this framework organizes cooperation. The EU does not seek to standardize its administrations; it seeks to make their interactions possible, predictable, and reusable. The European portal also emphasizes the importance of identifying needs, experimenting with solutions, and then deploying those that can be reused on a large scale. The solutions recommended by the Board are selected based on their usefulness to users, their reusability, their security, their data protection, their openness, and their sustainability. In other words, European governance of interoperability is based on a framework of consensual common standards and selective pooling, rather than on a framework of centralized control.

3.4 The Australian case: strategic integration of capabilities

The Australian experience is also instructive, but for slightly different reasons. Australia has explicitly integrated data interoperability, digital security, and the citizen experience into a single path towards government modernization. Its Data and Digital Government Strategy sets out a vision for 2030: to deliver simple, secure, and connected public services, using world-class data and digital service capabilities.
In its implementation documents, the Australian government states that secure data exchange supports interoperability, the reduction of duplication, reliable information flows between public bodies, and an improved user experience. The Australian public architecture thus directly links trust, efficiency, and interoperability.

3.5 Concrete tools to build trust

Australia has also reinforced this approach with more specific tools. The government has stated that the Digital ID Act 2024, effective from 1 December 2024, establishes consistent national standards for identity verification to make online interactions simpler and safer for individuals. The same set of public policy tools emphasizes that increased data-sharing capabilities must be accompanied by robust safeguards for privacy, security, and public trust.

3.6 The role of jurisdictions in the federated framework

Furthermore, the consultations leading up to the Australian strategy show that the states and territories themselves have called for greater two-way data sharing, common national approaches, and shared infrastructure to improve services for citizens. This combination is significant: it demonstrates that federated governance can be driven not only by the centre, but also by the participating jurisdictions when they see a tangible benefit for individuals and for the effectiveness of public action.

3.7 The structuring role of APIs and standards

Australia also offers valuable insights into the role of APIs, reuse standards and the ‘tell us once’ principle. Its public strategy states that application programming interfaces must promote efficiency, reuse, risk reduction, and interoperability between systems, whilst supporting the transition to more seamless services for users. This approach ties in directly with the idea, already present in previous CIRANO work, that the pooling of resources should not be viewed as a merger of administrations, but as a shared capacity to circulate information in a secure, governed, efficient and useful manner.

3.8 The OECD's analytical contribution

Beyond these two examples, the OECD provides a particularly useful framework for understanding the issue. The organization emphasizes that access to and sharing of data can maximize the social and economic value of data reuse, whilst requiring governance frameworks capable of balancing benefits and risks.

The OECD also points out that governments play a decisive role in the development of digital public infrastructure, the key components of which include digital identity, data sharing, core registers, and mechanisms for ensuring consistency between systems. In other words, the converging international literature no longer presents data circulation as a peripheral issue; it treats it as a prerequisite for state performance, trust, and capacity.

Beyond the institutional frameworks analyzed, a complementary dimension deserves explicit consideration: that of international data-sharing platforms and transformative transnational initiatives. In several strategic areas, payment systems, climate transition, biodiversity, health and risk disclosure, coordination mechanisms based on common standards and shared data infrastructures are being rolled out internationally. These initiatives are not limited to technical cooperation exercises: they actively contribute to defining the standards, protocols and governance models that shape global digital ecosystems.

Canada's ability to participate credibly in these dynamics depends in part on its own internal coherence. A federated interoperability framework at the FPT level is not merely a lever for domestic efficiency; it also becomes an instrument of strategic positioning, enabling Canada to contribute to the development of international standards and to capitalize on the lessons learned from these platforms.

This approach offers a significant operational advantage. Experience shows that alignment with international standards and frameworks can facilitate coordination between domestic jurisdictions by providing neutral and recognized points of reference. It also helps avoid exclusive reliance on external models, positioning Canada not only as a user but also as an active contributor to the evolution of international frameworks.

3.9 Conditions for the success of a federated model

International experience does not argue in favour of either data centralization or mere ad hoc collaboration between administrations. It shows that a federated model can work when four conditions are met: a stable policy direction, shared and adaptable standards, mechanisms for trust and compliance, and a governance capacity capable of identifying, selecting, and reusing relevant solutions.

3.10 Transition to operationalization

These lessons do not point to a single model, but to an adaptable architecture. It is precisely this architecture that the following section translates into an operational prototype within a Canadian FPT context, building on the insights already set out in previous CIRANO publications and converging public policy developments.

Section 4. From a conceptual prototype to an operational basis for FPT discussion and negotiation

The transformations analyzed in the preceding sections, whether the restructuring of digital infrastructures, the hardware constraints associated with AI, or the growing implications for national security, converge on a common observation: the state's capacity for action now depends on its ability to coordinate, at the system level, assets that remain institutionally distributed.

In this context, the formalization of a federal–provincial–territorial framework agreement on the interoperability of public data and the adoption of artificial intelligence is no longer merely a forward-looking exercise. It can now be envisaged as an operational step, made possible by the convergence of existing frameworks, sectoral initiatives and evolving political will.

The preliminary draft agreement drawn up during the preparatory work for this document provides a structured framework in this regard, drawing, in particular, on recent developments in Canada and internationally**,** whilst being explicitly tailored to the characteristics of Canadian federalism. To be useful at the decision-making level, however, this prototype must be read as an advanced working document, intended to structure actual intergovernmental negotiations, and not as a finalized or prescriptive legal text. Its value lies precisely in its ability to make tangible the available options, the necessary trade-offs, and the concrete implementation arrangements.

4.1 A federated vision: achieving interoperability without centralisation

As a direct extension of this observation, the prototype proposes a renewed interpretation of interoperability, adapted to the structural constraints of Canadian federalism. At the heart of the model lies a key conceptual proposition: interoperability is based neither on the centralization of data nor on its widespread sharing, but on the establishment of a federated ecosystem founded on common rules, trust mechanisms, and targeted exchange capabilities.

This distinction is essential in the Canadian context. It makes it possible to reconcile two imperatives often perceived as contradictory: on the one hand, the preservation of jurisdictions and jurisdictional control over data, and, on the other hand, the growing need for intergovernmental collaboration to address systemic challenges, whether in service delivery, national security, or the use of artificial intelligence capabilities. Conceived in this way, the framework agreement does not aim to harmonize existing systems, but to create the conditions for their interoperability, through the gradual definition of common protocols, standards and institutional mechanisms, the adoption of which remains adaptable to the realities of the participating jurisdictions. This approach allows interoperability to be viewed not as an external constraint, but as an emerging capability of the system itself.
This federated approach also helps to limit the risks of excessive concentration and technological dependence by avoiding the creation of single points of failure and by maintaining a distribution of capabilities across jurisdictions.

4.2 Foundational principles adapted to Canadian federalism

This federated vision is operationalized through a set of guiding principles that provide a framework for action without predetermining its specific arrangements. The prototype agreement is thus based on principles that constitute the conditions for its political and operational feasibility. These principles, a focus on people, citizens, and users; data reuse based on the 'once-only' principle; openness; security; proportionality; accountability; and jurisdictional sovereignty, define a balance that is operationally realized through mechanisms for supervised data sharing between jurisdictions.

In practice, this balance relies on the ability of jurisdictions to organize a targeted pooling of certain functions, standards, and collaboration mechanisms, without transferring control over the data itself.

One of the most significant contributions of the proposed model lies in the combination of three complementary approaches:

- a voluntary approach, allowing jurisdictions to join according to their priorities.
- a modular approach, allowing for sector-specific or use case-based rollouts.
- an evolutionary approach, recognizing the need for a gradual transition from existing systems.

This triptych of voluntarism, modularity and progressivity represents a crucial lever for acceptability. It enables the envisaging of an adaptable implementation that takes into account differences in institutional capacity and varying priorities within governments. It also establishes the minimum conditions for sustainable collaboration over time.

4.3 A governance architecture geared towards collaboration and execution

On this basis, the question of governance no longer arises in terms of the formal distribution of powers, but rather the effective capacity to coordinate action. The prototype proposes a governance architecture structured around a central-provincial-territorial (CPT) collaboration mechanism responsible for supporting strategic alignment, consistency of approaches and monitoring of implementation.

This structure, which may take the form of a Board or a collaborative forum, is supported by secretariat functions, specialized technical committees, and designated points of contact in each jurisdiction. It aims to ensure a capacity for ongoing collaboration, whilst remaining adaptable to the organizational choices of the participating governments.

The proposed link with the new Digital Transformation Office at the heart of the federal government is a key structural element, in that it would enable the functions of governance, standardization and implementation support to be aligned, without altering the specific responsibilities of each jurisdiction.

Beyond its institutional structure, this framework introduces a significant development: it transforms ad hoc collaboration mechanisms into a structured capacity capable of supporting more consistent intergovernmental action over time, a prerequisite in an environment characterized by rapid technological change. In particular, this architecture enables the introduction of a capacity for sharing knowledge and experience that is essential for anticipating the effects of interdependence between systems and reducing the risks of failures spreading across interconnected networks.

4.4 A transformative innovation: interoperability assessment

From this perspective, the coherence of the system cannot rely solely on ex post mechanisms; it also requires tools that enable action to be taken at an early stage.
Among the most fundamental elements of the prototype is the introduction of a mechanism for assessing the interoperability of value-added data, applicable to initiatives likely to impact data exchanges between jurisdictions in strategic sectors.
Drawing, in particular, on international practices, this mechanism aims to encourage public authorities to anticipate the effects of their decisions, whether legal, technical, or organizational, on the overall interoperability of systems. It is part of an ex-ante consistency approach, helping to limit the emergence of incompatible solutions and reduce the costs associated with fragmentation.
Beyond its technical function, this mechanism constitutes a powerful collaborative risk management tool. By promoting ex ante analysis of impacts on interoperability, it enables the early identification of potential vulnerabilities, critical dependencies and systemic effects that may arise from isolated decisions. In the Canadian context, such an approach introduces common benchmarks that can support decision-making, whilst respecting the processes specific to each jurisdiction.

4.5 Operational tools: supervised experimentation and exchange agreements

The practical application of these principles and this governance framework, however, rely on tools capable of supporting action at the operational level. The envisaged framework is therefore not limited to defining general guidelines; it provides for mechanisms enabling gradual and controlled implementation.

Interoperability sandboxes enable solutions involving multiple jurisdictions to be evaluated in secure environments, in order to assess their implications prior to wider deployment. They also play a key role in reducing uncertainty by allowing interactions between systems to be assessed in controlled environments before any wider roll-out, thereby limiting the risks of unforeseen effects on a large scale.

At the same time, data-sharing agreements serve as key mechanisms for translating general principles into operational procedures tailored to specific use cases. Guided by parameters relating to purpose, legal basis, security, governance, and accountability, they offer a flexible framework for reconciling innovation with risk management.

This interplay between experimentation and progressive contractualization enables intentions to be transformed into concrete capabilities, without compromising control over the systems.

This approach to structured experimentation is particularly relevant in contexts requiring approaches tailored to institutional and cultural realities. The diversity of governance frameworks, priorities, and practices specific to First Nations makes a uniform approach to data interoperability and the adoption of artificial intelligence difficult. In this context, a strategy based on targeted pilot projects appears more appropriate than widespread integration from the earliest stages.

Such an approach would allow for experimentation, within defined environments and in close collaboration with the communities concerned, with data governance models that respect the cultural, institutional, and legal contexts specific to each nation. It would also provide a space for mutual learning, for both public administrations and indigenous partners, with a view to gradually developing appropriate frameworks based on trust, reciprocity, and recognition of specificities.

4.6 A gradual and adaptable implementation

The effectiveness of this framework, however, depends on its ability to be realistically deployed within a complex institutional environment. The prototype therefore envisages an implementation approach based on differentiated pathways, taking into account the priorities, capacities, and constraints specific to each jurisdiction. This approach can be supported by common roadmaps, specific action plans and monitoring mechanisms based on shared indicators, with a view to collective learning and continuous improvement.
Periodic review and adjustment processes enable the framework to be adapted to technological, organizational, and strategic developments, recognizing that interoperability is an evolving process rather than a final state. Monitoring and continuous improvement mechanisms help to maintain the ability to adapt to evolving technological and organizational risks, whilst preventing the system from becoming rigid.

4.7 Legal safeguards and respect for competences

This progressive approach ultimately requires a sufficiently clear legal framework to underpin trust between the parties. The agreement therefore includes explicit safeguards designed to ensure its compatibility with the Canadian constitutional framework and existing legal regimes. These safeguards also help to mitigate the risk of losing decision-making control by ensuring that the systems deployed remain anchored within explicit and verifiable legal frameworks.
The participation of the jurisdictions does not entail any changes to their powers, and the implementation arrangements must be interpreted in the light of applicable laws, particularly regarding privacy protection, access to information and data management. These safeguards are essential to ground the agreement in a spirit of collaboration that respects each party's responsibilities, and to support the gradual adoption of the agreement by the relevant authorities.

4.8 A discussion framework directly applicable to action

Taken as a whole, the prototype constitutes a federated and coherent architecture, covering the legal, technical, organizational, and economic dimensions of interoperability.
Its value lies in its ability to move beyond a strictly conceptual approach to offer a working framework that can be directly applied in an intergovernmental context. It enables a structured discussion on implementation arrangements, whilst leaving open the options regarding the pace, scope, and mechanisms of participation.

It thus builds on the transformations analyzed throughout this document: these point not only to the need for better collaboration, but also to the emergence of a collective capacity to act in a more integrated manner. The proposed architecture is neither a formal proposal nor a recommendation at this stage. It aims to provide a sufficiently structured working framework to support informed intergovernmental deliberation.

For deputy ministers and decision-makers, this prototype offers a concrete starting point for moving current exchanges towards more coordinated approaches, without prejudging the final choices that will be determined by the negotiation process. In an environment where the ability of public administrations to utilize their data in a coherent manner is becoming a key determinant of their effectiveness, resilience, and decision-making autonomy, such an instrument appears less as an institutional innovation than as a progressive response to the contemporary demands of public action, and as a foundational step towards an integrated strategic capacity. This project also helps to position Canada as a credible player in the international dynamics of data governance, by facilitating its alignment with and contribution to emerging standards.

Conclusion

From feasibility to decision: towards an explicit FPT negotiation mandate

The analysis presented in this document leads to a conclusion that is now difficult to dispute: Canada is no longer in an exploratory phase, but at a tipping point.
The conditions that, just a few years ago, made the interoperability of public data difficult to envisage at the federal-provincial-territorial level no longer prevail. A strategic vision for artificial intelligence has now been formulated. Concrete applications are being rolled out across government departments. A credible institutional precedent for digital cooperation has been established with the Kananaskis Agreement. Standards, architectures, and technical capabilities have reached a sufficient level of maturity.
In other words, the building blocks of an integrated capacity for action are in place. What remains unresolved is not their relevance, but how they are brought together.

The central issue is no longer conceptual. It has become a matter of decision-making. The absence of a structuring framework for interoperability is no longer simply an organizational shortcoming. It is becoming a factor of fragmentation that limits the scope of public investment, slows the adoption of artificial intelligence on a large scale, and reduces the ability of governments to act coherently in the face of systemic challenges. It also leads to a dilution of efforts, a duplication of investments and a loss of collective leverage. Beyond its institutional implications, this capacity directly determines the quality of services offered to citizens, the protection of their rights in a digital environment, as well as their security, prosperity, and quality of life.

Conversely, the implementation of an FPT framework agreement would make it possible to transform what is still only partial convergence into operational capacity. It would provide a concrete mechanism for linking existing initiatives, guiding future investments and supporting a gradual yet structured ramp-up of public data interoperability in Canada. The prototype proposed in this document should be viewed in this light. It is neither a fixed model nor a prescriptive proposal. It aims to give tangible form to an option that is now credible: that of an operational federalism capable of organizing the secure, governed, and useful flow of data, without calling into question jurisdictional responsibilities.

Its value lies precisely in its ability to shift the discussion from a widely accepted diagnosis towards a structured debate on the practicalities of implementation. Consequently, the question facing public decision-makers becomes clear: how can we organize, within a federated framework, the conditions that will enable public data to fully support the transformation of services, the effectiveness of public action and the country's digital sovereignty? Answering this question is no longer merely an additional analytical exercise. It involves initiating a genuine collaborative process, based on explicit choices regarding governance, standards, incentives, and implementation priorities.

From this perspective, the issue becomes explicitly political: authorizing the opening of a formal negotiation forum at the federal-provincial-territorial level. A first concrete step would be to entrust a clear mandate to the relevant authorities, responsible ministers, deputy ministers, and chief information officers, to structure this transition: collectively evaluate the proposed prototype; identify priority use cases with high impact; define a shared collaboration framework, including rapid experimentation mechanisms; and specify the parameters of a potential framework agreement on governance, standards and incentives.

Such an approach can be initiated without delay, in a pragmatic and incremental manner, building on existing intergovernmental mechanisms. It requires neither a major institutional overhaul nor prior harmonization of systems but is based on an explicit commitment to organizing their interoperability. This approach is not without precedent. Recent experience in the field of cybersecurity has shown that federal, provincial, and territorial governments are capable of acting collectively when the issues are recognized as strategic and the conditions for collaboration are clearly established.

Data interoperability is now the logical next step in this trajectory. The risks associated with data integration and artificial intelligence are not downplayed. On the contrary, they form a key element of strategic thinking. But these risks do not stem from interoperability itself: they result from the lack of a framework. A fragmented system does not reduce complexity; it displaces it, conceals it and, ultimately, succumbs to it. It does not limit dependencies; it succumbs to them. It does not protect the capacity for action; it hinders it. The challenge is, therefore, not to slow down the linking of strategic data in the sector in Canada, but to structure it.

The proposed framework agreement precisely provides this structuring. By introducing mechanisms for governance, evaluation, experimentation, and oversight, it enables diffuse risks to be transformed into manageable variables and imposed complexity into a steered capability. In an international environment marked by technological acceleration and the realignment of power dynamics, the ability to organize, understand and govern data systems is becoming a key determinant of sovereignty. In this regard, regulated interoperability does not constitute an additional risk. It is the prerequisite for mastering them.

Inaction is no longer a neutral option. It entails a growing cost in terms of inefficiency, fragmentation, and loss of collective capacity."
Consequently, the question is no longer whether action should be taken, but when and in what form such action should be undertaken. Delaying this step would amount to prolonging a situation where capabilities exist without being fully mobilized, at the increasing cost of systemic inefficiencies and missed opportunities. Conversely, launching a mandate for negotiations, even one limited in its initial scope, would help to structure a common space for action, accelerate collective learning, and set Canada on a coherent path towards transforming its public sector.

In an environment where states' ability to harness their data is becoming a key determinant of their performance and strategic autonomy, inaction now carries a growing cost, often invisible in the short term but structuring in the long term. Conversely, a coordinated approach would enable Canada to secure a sustainable comparative advantage: that of a public system capable of functioning as a coherent whole. The current situation does not guarantee the success of such an approach. But it does make it possible. The challenge is no longer to produce data, but to organize it so that we can act collectively, effectively and in a timely manner.

This is precisely what makes this a decisive moment.
It now calls for a decision by the governments of the federation.

Appendix, Working framework for a federal-provincial-territorial instrument on data interoperability and the responsible adoption of AI

The following text presents a structured working framework designed to illustrate, in concrete terms, the parameters that a federal–provincial–territorial instrument could bring together to support public sector data interoperability and the responsible adoption of artificial intelligence in Canada.

Developed on the basis of existing practices regarding intergovernmental agreements in Canada and informed by certain recent international developments, this working framework proposes a federated architecture covering the dimensions of governance, standards, data sharing, security, implementation, and monitoring. It aims to clarify the operational, legal, and organizational trade-offs associated with such an instrument, whilst respecting the legislative frameworks and specific jurisdictions of each jurisdiction.

This working document is neither a formal proposal nor a finalized text. Its deliberately advanced structure is intended to allow for a realistic assessment of the implementation arrangements, including collaboration mechanisms, interoperability requirements, and incentive mechanisms. It remains open to adjustments, particularly regarding the degree of constraint, financing mechanisms, asymmetry provisions, and membership arrangements.

The document is presented in a format similar to that used in FPT agreements in order to facilitate its uptake by the relevant administrations and to support, where appropriate, exploratory, or preparatory work. The elements contained therein may be adapted, adjusted, or sequenced according to the priorities of the participating governments, including differentiated approaches by sector or by jurisdiction.

This working document may be read selectively. Its primary aim is to provide a common basis for examining, in an informed and pragmatic manner, the conditions under which an interoperable capability at the FPT level could be progressively established, in line with the guidelines already identified and the operational constraints of public administrations. It is presented for discussion purposes and in no way prejudges the positions that participating governments might adopt in a formal negotiating framework.

PREAMBLE

- This text seeks to organize, for the purposes of discussion, the key elements of a federal–provincial–territorial instrument ("the Parties") aimed at promoting the interoperability of public data and the informed implementation of artificial intelligence. The Parties agree that data represents a crucial strategic asset for ensuring the optimal delivery of public services, for developing policies and for strengthening governments' capacity to act. They also recognize that each jurisdiction has its own jurisdictions and legal frameworks.
- The Parties recognize that artificial intelligence constitutes critical infrastructure supporting the digital transformation of the public sector.
- The Parties wish to promote a high level of interoperability in the public sector in Canada, enabling secure, reliable, and transparent data sharing.
- the Parties recognize the division of powers within the Canadian federation as well as their respective legal frameworks, particularly with regard to privacy protection and access to information.
- the Parties recognize existing strategies on data, digital technology, and artificial intelligence at the federal, provincial, and territorial levels.
- the Parties recognize the importance of trust, data sovereignty, including that of Indigenous data, and responsible governance.

In this context, it seems useful to specify the general parameters that could structure such an approach, so as to facilitate its review and, where appropriate, its gradual adoption.

ARTICLE 1 , PURPOSE AND SCOPE

The document establishes a common framework aimed at promoting the interoperability of public sector data; supporting the development of intergovernmental digital public services; facilitating administrative, analytical and decision-making cooperation; enable the coordinated development of artificial intelligence infrastructure; reduce duplication and improve the efficiency and quality of public services; protect privacy, security and individual rights; and respect data sovereignty (including the governance of Indigenous data), where applicable

The envisaged mechanism applies to participating public bodies of the Parties and covers both personal and non-personal data, subject to applicable laws. It promotes the sharing and reuse of data and systems. It enables the establishment of intergovernmental digital public services (for example, a 'one-stop shop' for accessing services across different jurisdictions). It ensures consistent standards (organizational, semantic. Technical, legal) and ensures governance, accountability, oversight, and dispute resolution. It establishes the general parameters that can provide a framework, in a progressive and adaptable manner, for intergovernmental cooperation on data interoperability and the responsible use of artificial intelligence in the public sector. Clarifying these parameters requires a shared understanding of the concepts involved, in order to ensure consistency in exchanges and interpretations between jurisdictions.

ARTICLE 2 , DEFINITIONS

For the purposes of this framework, the following definitions are proposed to facilitate a common understanding of the concepts used, whilst allowing for their adaptation to the specific legal and operational contexts of the participating jurisdictions:

- 'Public sector bodies', ministries, agencies, institutions, and statistical bodies under the jurisdiction of the federal government, provinces, and territories.
- "Interoperability solution": a specification, standard, interface, component, service, or architecture that promotes interoperability (technical, semantic, organizational, and legal).
- 'Interoperability assessment': a formal assessment of a binding requirement, in order to evaluate the impact on interoperability.
- "Structural requirement": any obligation, prohibition, condition, criterion, or limit (legal, regulatory, technical, or organizational) affecting digital public services or the exchange of data between jurisdictions.
- "Interoperability sandbox": a controlled environment facilitating the prototyping and testing of interoperability solutions in a collaborative context.
- "Data exchange agreement" or "Data sharing agreement" , a formal agreement concluded under this framework for the transfer or sharing of data between parties.
- "Data Management and Governance Framework" , policies, roles, responsibilities, oversight, metadata, access, etc.

This instrument also applies the technical definitions included in the "OECD Board Recommendation on Improving Access to and Sharing of Data," to which Canada adheres.
Beyond the definitions, the harmonization of approaches is based on a set of common principles that can guide choices without predetermining the specific arrangements.

ARTICLE 3 , PRINCIPLES

The principles set out below are intended to guide the potential implementation of an interoperability framework by providing common benchmarks to inform decisions, without prejudging the specific arrangements adopted by each jurisdiction.

Interoperability is user-centred, promoting the principle of once-only data collection and data reuse, where permitted by law. Solutions prioritize openness, transparency, and reuse, whilst respecting security and confidentiality requirements.

The Parties shall collaborate on standardization, data quality, and the use of shared and adaptable standards, whilst applying the principles of proportionality and data minimization. Only data necessary to achieve the objective shall be shared.
The least intrusive method must be used (for example, pseudonymization, anonymization where possible).

Each Party remains responsible for its own actions and must ensure that exchanges are traceable, auditable, and transparent. Artificial intelligence systems are subject to proportionate assessment and approval mechanisms. An AI system that has been audited and approved in a province is subject to a fast-track procedure for use in federal agencies, thereby reducing the regulatory scrutiny that currently slows its deployment.

The proposed instrument respects data sovereignty and jurisdictional autonomy. The principles of Indigenous data sovereignty must be respected in relevant contexts. The Parties may adopt separate solutions provided they ensure equivalent results in terms of interoperability.

The approach adopted is progressive, evolutionary, and based on intergovernmental cooperation. The Parties recognize that interoperability generates efficiency gains that can be reinvested in the modernization of public systems. Interoperability must not compromise privacy or security. Data sharing must comply with the Privacy Act (federal), provincial/territorial privacy laws, and/or applicable legislation. Decisions regarding national standards and data frameworks are made by consensus.

The parties undertake to coordinate governance, resolve conflicts, and make joint decisions on standards, changes, upgrades, etc. Translating these principles into practice requires appropriate collaboration mechanisms to ensure their operationalization in an intergovernmental context.

ARTICLE 4 , GOVERNANCE

This section describes an indicative governance structure designed to support intergovernmental collaboration, whilst allowing participating jurisdictions the necessary flexibility to adapt their participation and internal mechanisms.

An FPT Interoperability Board is established by the agreement of the Parties:

- It is composed of representatives of the federal, provincial, and territorial governments (including Indigenous partners), as well as observers and technical advisers. It is governed by a permanent co-chairmanship: one held by the federal government, the other by a representative of the provinces and territories (appointed on an annual rotation basis).
- The Board serves as a joint coordination body, aiming to facilitate strategic alignment and consistency across initiatives. It facilitates and coordinates the direction and implementation of the FPT framework for public sector data interoperability in Canada: it contributes to the development of common consensus-based standards; resolves disputes; updates the interoperability framework; supports monitoring; and coordinates funding and investment.
- The Board provides the Parties with a reliable forum for sharing knowledge and experiences relevant to its mission.
- The Board is not an advisory body. It acts as a body for coordination and strategic alignment. It has no binding decision-making power over the participating jurisdictions, whose autonomy is fully preserved.

- The Board is supported by a secretariat responsible for administrative and technical support, shared mechanisms, directories accessible to the parties, shared registers, metadata catalogues, interfaces, and portals.
- **The secretariat** establishes and maintains a common repository of interoperable solutions, approved standards, reusable components, APIs, schemas, and ontologies.

The proposed Digital Transformation Office and the Federal-Provincial-Territorial Board for AI Adoption and Data Interoperability have complementary mandates focused on modernizing the delivery of public services through technology and data. Each participating public body designates a single point of contact responsible for coordinating interoperability issues, consulting with other jurisdictions and managing implementation at the local level.
FPT technical committees are established to:

- the voluntary convergence of semantic and interoperability standards, security and privacy, and emerging technologies; the authorization, monitoring and evaluation of interoperability sandbox projects and sectors of activity (health, environment, etc.)
- Feedback and joint reviews of interoperability, structural requirements, and their cross-jurisdictional impact.

A framework for such collaboration also requires the identification of technical and organizational components capable of supporting the gradual convergence of systems.

ARTICLE 5 , INTEROPERABILITY FRAMEWORK
The elements presented in this section illustrate the possible components of a common interoperability framework, including standards, tools, and collaboration mechanisms, with a view to gradual and non-prescriptive convergence.
The Parties shall collaborate on the development and gradual adoption of common standards covering technical, semantic, organizational, and legal aspects; a shared register of standards, solutions and components shall be maintained.
In this context, it is important to consider mechanisms for anticipating and managing the impacts of regulatory and technological developments on interoperability

ARTICLE 6 , INTEROPERABILITY ASSESSMENTS
This section proposes an assessment mechanism designed to support intergovernmental consistency in initiatives affecting interoperability, whilst respecting the decision-making processes specific to each jurisdiction.
Interoperability assessments and shared convergence standard
Where a jurisdiction is planning a major legislative or technical change (legal, regulatory, technical, or organizational) that is likely to impede the exchange of interoperable data or digital public services between jurisdictions (i.e., FPT or multi-jurisdictional services), it may, where relevant, conduct a convergence assessment.

The assessment takes into account legal, regulatory and policy constraints; the technical and semantic implications of interoperability; the implications for organization, administration, and processes; the implications for reuse, costs, and duplication across jurisdictions; risks to privacy, security, and confidentiality; and possible mitigation measures (alternatives, exceptions, transition pathways).

This assessment may be shared with the Interoperability Board to facilitate consistency and identify potential interoperability issues with FPT partners. Rather than imposing a single rule, the assessment proposes 'interoperability bridges' to maintain data flow without interfering with the province's legislative autonomy.

The Interoperability Board may make recommendations aimed at facilitating interoperable compatibility. In some jurisdictions, this may be linked to regulatory impact assessments or legislative review processes. The parties undertake to publish summaries of the assessments (transparency), excluding sensitive information.
Alongside these assessment mechanisms, experimental approaches may help inform future choices within a controlled framework.

ARTICLE 7 , INTEROPERABILITY SANDBOXES

The following provisions set out a regulated approach to experimenting, in a controlled and reversible manner, with interoperability solutions, with the aim of informing future choices without creating immediate obligations.

- A sandbox is a controlled environment for prototyping, testing, and validating new interoperability solutions (technical, semantic, legal) involving one or more jurisdictions under regulated supervision.
- Parties may submit a proposal to the Board. Criteria include minimal risk, clear objectives, a defined duration, an exit strategy, privacy safeguards, and an interoperability impact plan.
- Sandbox projects are subject to collaborative monitoring and periodic reporting to the Board. Where personal data is involved, review by the relevant data protection authorities or supervisory bodies is required.
- Where a sandbox solution proves successful, it may be elevated to the status of a fully fledged interoperability standard (following due assessment and approval).
- Participants remain liable for their actions under applicable law. The agreement must specify liabilities, indemnities, and remedies.

The lessons learnt from these experiments can then be translated into concrete arrangements for data exchange between jurisdictions.

ARTICLE 8 , DATA EXCHANGE AGREEMENTS

This section describes the general parameters that may govern the conclusion of data-sharing agreements between jurisdictions, with a view to ensuring consistency with the principles of the framework whilst complying with applicable legal obligations.

In this context, when two or more parties exchange data, they may enter into a data exchange agreement (DEA) (or data-sharing agreement) that implements the principles of the proposed FPT framework.
Each DSA specifies:

- the purpose and use , defining the purpose(s) for which the data may be exchanged or reused,
- the scope and types of data , what are the data elements, datasets, and metadata?
- The legal basis and consent, references to the statutory authority, whether or not consent is required, and conditions.
- Security and protection rules, standards, encryption, access controls, and audit logs
- Anonymization, pseudonymization, or de-identification, where applicable.
- Obligations regarding data retention, deletion, and archiving
- Functions and obligations: the roles of the sender, recipient, administrator, custodian, and governance
- Quality, standards, and interoperability , commitments to use common vocabularies, schemas and metadata, quality rules
- Liability and indemnification
- Audit, logging and monitoring
- Dispute resolution/escalation
- Termination and exit strategy
- Modification, versioning, and migration
- Publication/Transparency , subject to confidentiality
- Intellectual property and licences (where applicable)
- Security incident management and breach notification

The implementation of such arrangements also raises considerations regarding funding, incentives, and the distribution of benefits.
The AED must also comply with the applicable privacy and freedom of information regimes in each jurisdiction.

ARTICLE 9 , FUNDING AND DIGITAL DIVIDENDS

The mechanisms set out below are presented for illustrative purposes; they represent various approaches that could support the implementation of an interoperability framework, particularly with regard to cost-sharing, incentives, and benefit-sharing.

- The signatories recognize that interoperability will generate digital dividends (economies of scale, reduced operating costs, accelerated service delivery).
- The federal government commits to converting a portion of national efficiency gains into computing credits, offering provinces coordinated and equitable access to distributed and shared computing capacity for their own AI projects.
- Local reinvestment: 40% of the administrative savings estimated using shared methodologies will be directly reallocated to participating jurisdictions to fund the modernization of their legacy systems.

Beyond the financial levers, the key issue remains that of the practical conditions for roll-out across the participating authorities.

ARTICLE 10 , IMPLEMENTATION

This section sets out a phased implementation approach, allowing participating jurisdictions to progress at their own pace, in line with their priorities, capabilities and operational constraints.

- Each Party shall draw up an implementation plan compatible with the shared collaboration framework, setting out the stages, resources, capacity building, and timelines.
- A shared collaboration framework (similar to the 'European Interoperability Agenda') to facilitate consistency in investment. Set priorities and promote convergence in the deployment of interoperability solutions.
- Regular reports (e.g., annual, or half-yearly) from administrations to the board on progress, measures, and gaps.
- Monitoring mechanisms are agreed between the parties on the progress of interoperability.
- Use of common performance indicators (KPIs) , for example, number of interoperable services implemented, number of cross-jurisdictional calls, reuse of components, cost savings, and user satisfaction.
- Mechanism for periodic feedback or joint peer review of compliance with the agreement's principles, governance, and technical obligations.
- A mechanism for amending the agreement (for example, by consensus or by an absolute majority of the parties) in order to respond to new technologies, new challenges, or new policy developments.

This implementation involves, in particular, structured management of the transition from existing systems.

ARTICLE 11 , SYSTEM TRANSITION

The following provisions aim to provide a framework for the transition of existing systems to interoperable environments, favouring pragmatic approaches based on compatibility, continuity, and risk management.

- Agreements on the transitional coexistence of existing systems, API/adapter wrappers, transition interfaces, conversion, and backward compatibility.
- Plans for the phasing out of non-interoperable systems.
- Budgeting for migration and re-engineering.

In this context, certain adjustments may be necessary to take account of the specific characteristics of different sectors of intervention.

ARTICLE 12 , SECTOR-SPECIFIC PROVISIONS

This section provides for the possibility of sector-specific adaptations, allowing for the specific characteristics of certain policy areas to be taken into account, whilst maintaining overall consistency.

- The envisaged interoperability framework may contain sectoral annexes (e.g., health, the environment, transport, education, and public safety) that incorporate standards, rules, vocabularies, and specialized governance specific to a particular field.
- With regard to health data, existing FPT initiatives on health data interoperability and management (e.g., the Shared Pan-Canadian Roadmap on Interoperability) would be integrated into this framework,
- For Indigenous data, special annexes recognizing the sovereignty of Indigenous data and joint governance agreements.

All of these elements must also comply with existing legal frameworks and obligations.

ARTICLE 13 , LEGAL SAFEGUARDS AND PRIVACY PROTECTION

The elements set out below are intended to ensure the framework's compatibility with existing legal obligations, particularly regarding privacy protection, access to information and respect for constitutional powers.

- Each party must ensure that its participation and obligations are consistent with its constitutional powers (federal and provincial).
- Participation does not override the statutory regimes of each jurisdiction (e.g. provincial privacy legislation, the federal Privacy Act, access to information).
- Data sharing must respect individual rights, control, consent, and regulatory oversight.
- Where personal data is involved, there are obligations regarding data breach notification, privacy impact assessments, and oversight by data protection commissioners.
- In the case of data flows between jurisdictions, conflict-of-law rules and harmonization are taken into account.
- The protection of sensitive or classified data, as well as exemptions and restrictions, are clearly defined.
- Jurisdictions may provide for exceptions or derogations (subject to justification) in certain areas.

In this context of voluntary cooperation, it is also important to provide for appropriate dispute resolution mechanisms.

ARTICLE 14 , DISPUTE RESOLUTION

This section proposes graduated dispute resolution mechanisms, inspired by existing intergovernmental practices and adapted to a context of voluntary cooperation.

Dispute resolution mechanism

- Stages: initial negotiation, mediation by the Board, referral to a higher authority or arbitration.
- In the event of a serious breach, temporary suspension of data exchanges or participation with a view to taking corrective measures.
- Liability and compensation: financial remedies or specific injunctions.

- Withdrawal: Provision allowing a party to withdraw from the agreement (with notice), and transitional obligations regarding data and interoperability assets.

These mechanisms take account of the diversity of situations and approaches among the participating jurisdictions.

ARTICLE 15 , ASYMMETRY AND FLEXIBILITY

The following provisions aim to explicitly recognize the diversity of approaches and capacities of participating jurisdictions, by allowing for differentiated implementation arrangements based on the principle of equivalence of results.

- The Parties may adapt implementation in accordance with their priorities.
- Any jurisdiction may adopt a separate solution ensuring equivalent results.
- Specific arrangements may be established

Finally, the sustainability and adaptability of such a framework depend on clear procedures for review and development.

ARTICLE 16 , FINAL PROVISIONS

This section sets out the general provisions relating to the duration, revision, and possible development of the framework, with a view to continuous adaptation.
The proposed framework shall enter into force upon signature for a fixed term; it is renewable.
It may be amended by mutual consent.
Any Party may withdraw from it by giving prior notice.

Sources and references (to be completed in APA style)

Natasha Tusikov, Blayne Haggart The Carney government's embrace of AI will put lives at risk. ***Policy Options*** *IRPP* 30 April 2026.