Foundations of Digital Sovereignty

Canadian Shield Institute

Foundations of Digital Sovereignty
Chapter 1 - May 2026

1

Contents

Contact:

Canadian Shield Institute
150 King St. West,
Toronto, Ontario, CA

canadianshieldinstitute.ca
info@canadianshieldinstitute.ca

Authors:

Vass Bednar
James McLeod
David Corbett
Emily Osborne
Kaylie Tiessen
Matthew da Mota

Photography:

Juan Rojas

Overview

Canada has spent decades ceding control of the digital economy to foreign private actors. Without a comprehensive governance framework, billions in new public spending on "sovereign" AI infrastructure will fail to deliver real sovereignty — and the window to act is now.

Compute spending without governance is money wasted. Canada must build the policy and institutional foundations first.

Key Takeaways

1. Where data is physically stored matters less than who owns the infrastructure and what laws they answer to. Under the U.S. CLOUD Act and FISA, American cloud providers can be compelled to hand over Canadian data regardless of where it sits.

2. Peer nations treat data regulation, IP protection, procurement, and technical standards as tools of national industrial policy and global competition. Canada treats them as neutral ground.

3. Canada ranks last in the G7 at converting R&D into commercialized products — our ideas succeed abroad, not at home.

4. A governance-first strategy requires three pillars: stronger legislation, modern public-interest institutions, and sovereign compute infrastructure.

Foundations of Digital Sovereignty will present a blueprint for building a meaningful strategy for sovereignty, ownership and prosperity in the digital economy:

- → How technical standards and international frameworks can be used strategically to advantage Canadian firms
- → Why Canada needs a national institution for intellectual property protection and research commercialization
- → Privacy legislation and sovereign data institutions, including a national data trust
- → The national security risks of Canada's dependence on foreign cloud hyperscalers
- → A procurement-led strategy for growing domestic cloud capacity
- → Antitrust enforcement, regulatory tools and blocking statutes as sovereignty instruments
- → Exploring potential options to build and operate Canada's sovereign compute infrastructure

Introduction

For roughly the past 40 years, the global economy has been undergoing a fundamental shift. We have moved from a world dominated by supply chains of tangible goods, to a world where intangible assets are the key driver of economic growth.

Canada has largely failed to respond to this evolution.

Most of the thorny problems that Canada faces today are a product of this central trend: Canada has surrendered governance and ownership of the digital realm. Indeed, we have allowed private actors — mostly foreign — to shape the rules of the digital economy, weakening Canadian sovereignty and giving rise to a litany of downstream problems that now characterize the digital economy's structure.

Privacy loss, fraud, low productivity growth, inescapable and compelling propaganda, polarization, child mental illness, cybersecurity risks, monopoly power, wealth inequality, and even democratic erosion are all downstream outcomes of Canada's fundamental failure to build institutions and governance structures that assert sovereign control over the digital realm.

What's more, this developing trend is currently being supercharged by artificial intelligence (AI) technology.

Foundational elements of AI technology were incubated in Canada, but due to our inattention to the realities of how value is created and captured, it was primarily American firms like OpenAI, Google, Microsoft and Anthropic that have successfully commercialized AI tools. We excelled at developing the underlying technology, but failed to design and deploy meaningful governance models.

Today, the Canadian government is already deploying billions of dollars as part of a Sovereign AI Compute Strategy, and as a country we are being asked to do even more to build up sovereign compute capacity.[1] Policy advocates and corporate interests say Canada must do this to compete in a global AI race where we are already barely playing catch up.

We are being told that Canada can leverage valuable data sources like public health records and financial data in order to assert a competitive advantage. But the solutions being put forward generally just amount to further reliance on foreign multinationals, with superficial claims of sovereign control.

In order to assert meaningful digital sovereignty, and to capture the economic benefits for Canada, we must do the hard work of developing and implementing an overarching governance framework.

A framework for governing AI, data and the intangible economy in the national interest will start with:

- Developing better legislative and policy instruments
- Building modern public-interest institutions
- Securing sovereign compute infrastructure

Without frameworks in place, the billions of dollars we spend on Canadian-resident compute capacity will do little to meaningfully strengthen Canadian sovereignty in the ways we care most about — bolstering economic prosperity, protecting privacy and governing society in accordance with Canadian values.

Investment in more computational capacity must be built on top of the foundation of a broader sovereignty strategy that affirms, protects and reclaims the value of data and information.

Before we blindly spend billions more on "sovereign" compute capacity alone, Canada must have clear governance and policy infrastructure in place to ensure that the economic value created by those new data centres is held by Canada and governed by Canadian values.

And just as importantly, we need corresponding institutions in place to ensure we are meaningfully governing the use of AI technology being deployed in Canada, regardless of whether it is operating on sovereign Canadian infrastructure or not.

Data Residency is Not the Primary Issue

Compute is the physical infrastructure that allows the digital economy to operate. And it can be tempting for policymakers to focus on the physical equipment as a way to simplify matters.

Unfortunately, this approach is very often misguided.

We have seen a long history of this misguided approach when it comes to Canadian data residency requirements. Essentially, data residency laws stipulate that Canadian government data must be stored in cloud infrastructure that is on Canadian soil. However, the U.S. CLOUD Act and the Foreign Intelligence Surveillance Act both permit the United States government to demand data from American cloud service providers — even if the data is not stored on U.S. soil.[2] Microsoft, in testimony to the French Senate, confirmed that it would not be able to refuse handing over data to the U.S. government — regardless of where the data was physically stored.[3]

Put simply**:** When it comes to sovereignty, where the physical infrastructure is located matters less than who owns the infrastructure and what laws they are subject to.

We see something similar when it comes to "sovereign" compute capacity. In the global artificial intelligence boom, one of the major constraints for companies is computation capacity. Policymakers worry that without access to "sovereign" compute capacity, Canadian companies that depend on compute will be at the mercy of multinational cloud service providers.

Faced with pressure to keep Canada in the global AI compute race, we've seen the government respond by stepping in directly with programs to try and build compute capacity to provide strategic access for Canadian researchers and firms.

In the 2024 budget, the federal government allocated $2 billion to the Canadian Sovereign AI Compute Strategy.[4] Months later, the government announced a $240 million plan to support Cohere, a Canadian generative AI company.[5]

But in reality, the deal was essentially government money helping Cohere secure computing capacity in a data centre being built in Cambridge, Ont.[6] However, the data centre was owned and operated by CoreWeave, a foreign firm.

Simply owning compute infrastructure is not enough; there needs to be an ability to govern inputs, outputs, operation and use cases associated with compute, and to ensure the retention of value produced by using that compute.

Even when data centres or AI firms are located in Canada, without clear, democratically-established rules, those firms will default to writing their own. That means operational policy will continue to follow corporate incentives and foreign regulations rather than the Canadian public interest.

In the two years since the Canadian Sovereign AI Compute Strategy was published, the pressure to secure sovereign Canadian compute capacity has only intensified. However, in those same two years, the government's proposed privacy and data reform legislation is once again stalled within Parliament.

Examples from other jurisdictions show that many different arrangements of compute ownership and location are possible in a sovereign compute strategy.

But in order for a country to thrive in the 21st century economy, a robust governance layer must exist over the infrastructure layer of compute. In particular, the governance of data is essential to successfully governing compute — both in terms of protecting data from misuse and mobilizing data for use in the public interest.

Canada's Failed Opportunity

Other countries have designed new regulatory frameworks to guide investment and acceptable behaviour by market participants. Those same frameworks create the conditions to help mitigate the downstream harms of digital systems.

By comparison, Canada has naively assumed that if we simply support research and development, good things will happen. Sadly, good things have not happened.

Canada has done a poor job of capturing the value-added economic activity created by our investments in R&D and intangible assets.

As a country, we've invested heavily in research and development at the university level.[7] We have one of the strongest and most dynamic research ecosystems in the world.[8] That system makes new discoveries and invents new technologies regularly, but we rank lowest in the G7 when it comes to turning innovation inputs like R&D into innovation outputs like commercialized products and value-added exports.[9]

In Canada, our main strategy has been to invest heavily in research and development at the post-secondary level and hope that the inventions created will magically be built into strong Canadian companies with commercialized innovations and IP ready to sell to a globalized world.

Instead, successive Canadian governments have worked very hard to attract foreign companies to operate in Canadian communities and partner with Canadian research institutions.

But we have a commercialization problem.

Canada is, famously, the country that incubated the researchers who ultimately made breakthroughs that led to the development of modern artificial intelligence technology.

The man venerated as the godfather of AI, Geoffrey Hinton, was ultimately hired by Google. More to the point, in spite of the significant AI talent incubated at Canadian universities, the biggest companies commercializing AI are almost all American.

It's not that our ideas don't become successful products, the problem is that the patents and other intellectual property is often registered to foreign firms and in other countries where the value add is captured by someone else. In many cases, government funded research is never even commercialized or turned into IP; novel discoveries are simply published as academic papers, and then left for any reader anywhere on earth to discover.

The most successful countries in today's digital age — such as the U.S., China, Germany and South Korea — have industrial policies to support the development and commercialization of sovereign technology, and economic development. Israel recognizes the value of public research and domestically developed IP, to the point that the country imposes export controls and requires repayment when valuable IP is acquired by foreign companies.[10]

Countries that create the conditions for prosperity and sovereignty tend to look at data regulation, standards development, research and development, government procurement, defence policy, and intellectual property protection as different spheres for competition and control.

Canada often treats these realms as neutral and democratic venues for co-operation, while other countries treat these systems as an opportunity to gain advantage.

Without a sharper strategy for governance and control, Canada's effort to build sovereign compute will fail to capture the economic value that comes from cutting-edge technologies, and we will continue to relinquish sovereign control through our own inattention.

Strategies for Sovereign Governance

While other countries have set strong rules and frameworks to guide investment in developing domestic companies and the infrastructure that they need, Canada has naively assumed that value-added activity would remain in country while ownership and commercialization happen elsewhere. Nothing could be further from the truth.

Building sovereign Canadian compute infrastructure is one important dimension. However, the government must also create the conditions for economic success — commercializing high-quality data and protecting privacy, capturing the intellectual property created by innovation, and embracing standards that advantage Canadian companies. Government must also be an anchor customer for promising Canadian companies to support them in scaling their technology.

Moreover, when Canada is more front-footed about governance in the digital realm, it will put the government in a better position to mitigate harms. Governance efforts can take place both through upstream inputs like data usage, and also by monitoring downstream outputs, such as child mental health issues.

Looking at peer jurisdictions, we can see examples of how Canada can start creating the structures of digital governance needed to assert real sovereignty over compute and AI systems. In the European Union, we have seen the government pass strong privacy and consumer protection legislation through the General Data Protection Regulations.[11] These rules include provisions for greater autonomy over personal data, restrictions on the collection of sensitive data, and interoperability and data portability requirements.

The EU AI Act also imposes a number of requirements for how data can be used in the development and deployment of AI tools, particularly restricting the use of biometric data and facial recognition technology (EU AI Act, Article 5).[12]

Strong legislative foundations for AI tools and privacy protection are essential for governing data.

Along with effective protection for data, the EU also has legal frameworks in place to mobilize data for the purposes of research and commercialization for the public good within the bounds of existing protections.

The EU's Data Governance Act seeks to enable secure and trustworthy data sharing and re-use to deliver benefits for citizens.[13] The law also supports the development of Common European Data Spaces — essentially data exchange and storage platforms to support the public interest and with embedded governance frameworks — in strategic sectors.[14] In particularly sensitive domains like health data, regulations like the European Health Data Space Regulation protect personal data, while also enabling its secure re-use for research and innovation in the public interest.[15]

More broadly, the Open Data Directive encourages EU member countries to make data resulting from publicly funded research open and available for re-use by default.[16] Estonia's X-Road model is an open-source data exchange platform connecting public and private sector databases, prioritizing work in the public interest and following the three requirements of interoperability, data integrity and privacy protection.[17]

On the other side of the globe, we see a similar mindset. South Korea's Data Accumulation Project, a part of the Data Dam project, seeks to accumulate and open data for the purposes of AI training, and create valuable jobs in the process.[18] European countries have also pursued statutes and other tools to impose strong controls on data and compute even when dealing with powerful monopolistic hyperscalers.

For example, Article 271 of the Swiss Criminal Code includes a blocking statute which in effect blocks the collection of evidence or information by foreign authorities for a foreign proceeding, preventing the circumvention of applicable Swiss rules on criminal, administrative, or civil proceedings.[19] The statute is particularly relevant in the context of banking since it makes it difficult for foreign insolvency offices to seek information on a debtor's assets from Swiss banks.

To achieve similar objectives, Israel's government used contractual requirements for American cloud service providers, namely Google and AWS, to sidestep legal obligations for extraterritorial access to secure the sovereignty of government data.[20]

A Blueprint for Digital Sovereignty

In 2025, the United States National Security Strategy explicitly articulated a geopolitical strategy that uses American technology platforms as an instrument of foreign policy and control.[21]

Taking a hard look at technology platforms and the terms of trade in the digital realm must be a top priority as Canada re-evaluates our relationship with the United States and our broader geopolitical strategy in a volatile world.

Canada needs a stronger and more comprehensive vision for governance of the digital realm. In subsequent chapters, Foundations of Digital Sovereignty will present a version of that vision.

First, we'll look at the building blocks of digital sovereignty: standards, intellectual property and data. Then, having established the foundational governance framework ideas for the digital realm, we will look at practical ideas for how Canada can build more sovereign digital systems, with strong governance embedded in the stack.

Chapter 2: Standards and International Frameworks

This chapter will examine the ways that other countries are able to use technology standards, international legal systems, trade agreements and other seemingly neutral systems to preference domestic firms and grow their own economies. In reality, these legal and technical frameworks can give competitive advantage to countries and companies, when they are used strategically.

By taking a more intentional and clear-eyed approach to technical standards, Canada can set our own terms for governance and technology development.

Chapter 3: Patents and Intellectual Property

Canada's geopolitical rivals see intellectual property generation and protection as a national imperative. International metrics consistently show that Canada underperforms on research commercialization. In a world economy where value is primarily derived from intangible assets, Canada needs a national institution for protecting and promoting comprehensive IP strategy.

Chapter 4: Privacy and Data

Data is the main factor for economic productivity in the intangible economy. The best strategy is for a country to develop regulations to protect individual privacy, preventing their data from being used in harmful ways, while also allowing proprietary data to be mobilized for economic value.

In this chapter we will look at privacy legislation and ideas for sovereign institutions like a national data trust to act as a steward for Canada's proprietary data.

Chapter 5: Risks to Canada's Cloud Infrastructure

Canada has neglected to assert strong governance in the digital realm, and that has put the country in a disadvantageous position. In the previous chapters, we've looked at how stronger governance strategy has contributed to economic success for competitors. In this chapter, we look at how Canada relies on foreign hyperscalers for cloud storage and computing infrastructure. This puts Canada in a subordinate position economically, but it also introduces direct national security risks — most notably from the U.S. CLOUD Act, and the Foreign Intelligence Surveillance Act.

Chapter 6: A Strategy for Growing Domestic Cloud Capacity

Having established the risks posed by ungoverned cloud infrastructure, this chapter will explore how Canada can secure the necessary cloud access for government, research and businesses while ensuring governance and privacy.

This chapter will look at the government's own cloud service needs, and how procurement can create anchor demand for growing the Canadian market for sovereign compute and cloud storage. With the right governance in place, the right technical standards, and a tiered approach to procurement, Canada can foster cloud infrastructure with a greater degree of governance, and greater economic benefits to Canada.

Chapter 7: Governance Tools for Canada's Digital Sovereignty

Even with better legislation and stronger public institutions, Canada will remain vulnerable to foreign manipulation and interference, in particular by foreign tech giants.

There are additional tools that Canada can use to assert control, without walling ourselves off from the world. Canada must aggressively develop and use tools that look outward and work to proactively protect itself in the international arena. Blocking statutes, trade negotiations, and antitrust enforcement can support Canada's efforts to secure its cloud.

Chapter 8: Building Sovereign Compute

To actually build sovereign domestic compute enabled by stronger governance, Canada can take multiple paths including partnerships with private industry as long as there are strong controls in place. Some of this capacity will need to be built and operated by the government and maintained as a public option for cloud and compute. This is especially true for government services, strategic research, and championing Canadian businesses through providing a secure, reliable, accessible, and affordable option.

This chapter will explore potential configurations for how Canada could build and administer our domestic compute capacity to meet these strategic needs, to invest in and develop next-generation compute to meet future needs rather than only trying to catch up with the current paradigm, and to ensure governance is embedded in these systems from the beginning.

Conclusion

The road ahead for Canada on digital sovereignty may seem daunting. The fact is that any serious effort to assert control and governance over the Canadian digital realm will be working to undo decades of inaction and complacency.

> "The old relationship we had with the United States based on deepening integration of our economies and tight security and military cooperation is over."
>
> — Prime Minister Mark Carney, 2025

The good news is that Canada is already navigating a moment of geopolitical volatility and realignment, and Canadians are broadly supportive of substantial efforts to bolster our national sovereignty.

The time is right, and as we will see in the upcoming chapters, Canada can borrow from peer nations to develop best practices for digital sovereignty and governance. We can do this.

References

1 Innovation, Science and Economic Development Canada, "Canadian Sovereign AI Compute Strategy," Government of Canada, last modified October 31, 2025, https://ised-isde.canada.ca/site/ised/en/canadian-sovereign-ai-compute-strategy.

2 CLOUD Act, P.L. No. 115–141, Division V (2018), https://www.justice.gov/criminal/media/999391/dl?inline; Andreas Kuersten, "FISA Section 702 and the 2024 Reforming Intelligence and securing America Act," Library of Congress, July 8, 2025, https://www.congress.gov/crs-product/R48592.

3 Senate of France, "Hearing of Mr. Anton Carniaux, Director of Public and Legal Affairs, and Mr. Pierre Lagarde, Technical Director for the Public Sector, of Microsoft France," June 10, 2025, https://www.senat.fr/compte-rendu-commissions/20250609/ce_commande_publique.html#toc2.

4 ISED Canada, "Canadian Sovereign AI Compute Strategy."

5 Department of Finance, "Deputy Prime Minister announces $240 million for Cohere to scale-up AI compute capacity," Government of Canada, December 4, 2024, https://www.canada.ca/en/department-finance/news/2024/12/deputy-prime-minister-announces-240-million-for-cohere-to-scale-up-ai-compute-capacity.html.

6 Canadian Shield Institute, *Sovereignty Score: Cohere Investment*, November 19, 2025, https://img1.wsimg.com/blobby/go/e37fd200-232f-4959-9dca-2108327c2abf/downloads/df90526f-3ef5-4182-8c82-1d0e889dc3fd/The%20Cohere%20Investment.pdf?ver=1775754443107.

7 The Daily, "Spending on research and development in the higher education sector, 2022/2023," Statistics Canada, November 1, 2024, https://www150.statcan.gc.ca/n1/daily-quotidien/241101/dq241101c-eng.htm.

8 Observatory of Economic Complexity, "Canada," accessed April 16, 2026, https://oec.world/en/profile/country/can.

9 Business Council of Alberta, "Canada's struggle to turn innovation into growth," October 6, 2025, https://businesscouncilab.com/insights-category/econminute/canadas-struggle-to-turn-innovation-into-growth/.

10 Israel Innovation Authority, "Royalties & Intellectual Property," accessed April 15, 2026, https://innovationisrael.org.il/en/royalties-intellectual-property/.

11 European Parliament and Council of the European Union, Regulation (EU) 2016/679 of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), [2016] Official Journal of the European Union L119/1.

12 European Parliament and Council of the European Union, Regulation (EU) 2024/1689 of 13 June 2024 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act), Official Journal of the European Union L 2024/1689, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32024R1689.

13 European Commission, "European Data Governance Act," accessed October 10, 2024, https://digital-strategy.ec.europa.eu/en/policies/data-governance-act.

14 European Commission, "Common European data spaces," accessed November 19, 2025, https://digital-strategy.ec.europa.eu/en/policies/data-spaces.

15 European Commission, "European Health Data Space Regulation (EHDS)," accessed April 16, 2026, https://health.ec.europa.eu/ehealth-digital-health-and-care/european-health-data-space-regulation-ehds_en.

16 European Commission, "European legislation on open data," last modified November 19, 2025, https://digital-strategy.ec.europa.eu/en/policies/legislation-open-data.

17 e-Estonia, "X-road – Interoperability services," accessed April 16, 2026, https://e-estonia.com/solutions/interoperability-services/x-road/.

18 Ministry of Science and ICT, "Data Dam project begins, being key to Digital New Deal," Government of South Korea, accessed April 16, 2026, https://www.msit.go.kr/eng/bbs/view.do?sCode=eng&nttSeqNo=453&pageIndex=&searchTxt=&searchOpt=&bbsSeqNo=42&mId=4&mPid=2.

19 Sandrine Giroud and Deborah Hondius, "Swiss Blocking Statute: update on do's and don'ts under the threat of criminal sanctions," Lalive, December 3, 2019, https://www.lalive.law/swiss-blocking-statute-update-on-dos-and-donts-under-the-threat-of-criminal-sanctions/

20 Harry Davies and Yuval Abraham, "Revealed: Israel demanded Google and Amazon use secret 'wink' to sidestep legal orders," The Guardian, October 29, 2025, https://www.theguardian.com/us-news/2025/oct/29/google-amazon-israel-contract-secret-code.

21 The White House, "National Security Strategy of the United States of America," Federal Government of the United States, November 2025, https://www.whitehouse.gov/wp-content/uploads/2025/12/2025-National-Security-Strategy.pdf.