5

Canadian Shield Institute

Foundations of Digital Sovereignty
Chapter 5 - June 2026

Clouds Without Borders: Why Data Residency Is Not Data Sovereignty

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:

Jason Ng
Juan Rojas
Caio Fernandes

Overview

For decades, Canadian policymakers have operated on the assumption that data residency is enough to guarantee Canada's digital sovereignty. That assumption is wrong.

Two pieces of U.S. legislation, the CLOUD Act and the Foreign Intelligence Surveillance Act, give American authorities the ability to access data held by U.S.-based cloud providers, regardless of where that data physically sits.

This matters for Canada, because three foreign hyperscalers dominate the Canadian cloud market — Amazon Web Services (AWS), Microsoft and Google.

As hyperscalers respond to growing demand for sovereign cloud with rebranded marketing rather than genuine governance solutions, Canada risks spending billions on infrastructure that does not actually protect the interests of all Canadians.

As we confront an increasingly volatile geopolitical landscape, Canadians are seeking to protect our national sovereignty. As we assess our vulnerabilities, Canada cannot ignore the reality that most of our digital infrastructure is both owned and controlled by foreign companies.

So of course, Canada should just build cloud infrastructure, right? But as we've already explored in previous chapters of *Foundations of Digital Sovereignty*, it is deeply misguided to rush out and spend billions of dollars on infrastructure, if we don't have a clear strategy for governance and economic value capture.

As we will see in this chapter, sovereignty does not depend on whether servers and data centres are physically located on Canadian soil. Governance is what matters, and Canada needs a clear strategy for meaningful governance of our digital systems.

Key Takeaways

1. Amazon Web Services, Microsoft and Google collectively hold roughly 63% of the global cloud market — and dominate the Canadian market similarly. Canada has very little autonomy over its own data when it sits with these providers.[1]

2. The U.S. CLOUD Act allows American law enforcement to access data stored by U.S.-based companies anywhere in the world. Microsoft confirmed to the French Senate that it could not refuse handing over data to U.S. authorities, regardless of where it was stored.

3. FISA Section 702 goes further — allowing warrantless surveillance of non-American persons by compelling data from U.S.-based cloud providers for broadly defined national security purposes. Canada's own government has identified FISA as the "primary risk" to data sovereignty.

4. "Sovereignty washing" is a growing problem: hyperscalers are marketing data residency as sovereignty while obscuring their fundamental legal vulnerabilities. Of cloud tools used by Canadian organizations that offer Canadian data residency, 88% remain exposed to the CLOUD Act.[2]

5. Governance must come before infrastructure. The $240 million Cohere investment — directed to a data centre built in partnership with U.S.-based CoreWeave — illustrates exactly what happens when spending outpaces governance.

The Cloud

Cloud services are typically provided through three service models:[3]

- Infrastructure as a Service (IaaS) affords the customer the greatest level of control over their computing environment, and includes many offerings from AWS, Microsoft and Google.
- Platform as a Service (PaaS) represents a blend between supplier and customer control, including examples like Google App Engine or Microsoft Azure App Service.
- Software as a Service (SaaS) offers ready-to-use applications that can be accessed over the internet. Familiar applications like Microsoft 365, Google Workspace or Dropbox are all examples of SaaS.

In spite of the imagery it evokes, cloud infrastructure is mostly about networking cables and warehouses full of racks of computing equipment. "The cloud" is a term used interchangeably to refer to a huge range of systems and processes — essentially all computing functions that are not handled locally on the device that you're using.

As an example, the government of Canada has complex and diverse computing requirements, which include a mix of storage, compute, and other cloud services. A scan through the list of approved cloud services available to the Government of Canada reflects this diversity, including everything from storage, networking, databases, developer tools, customer relations management, analytics, and AI and machine learning.[4]

Canadian companies have a similar array of needs, depending on their size and sector.

Amazon Web Services, ChatGPT, and YouTube all provide cloud services, but each of these services will have their own characteristics, infrastructure requirements and different governance requirements.

This is why, as we have already illustrated in the previous chapters of *Foundations of Digital Sovereignty*, our governance efforts must be focused on upstream factors — data, intellectual property and governance frameworks, like technical standards.

When looking at the current state of play in Canadian cloud capacity, one vulnerability comes into sharp focus: our reliance on foreign service providers.

Cloud Security

Three American cloud service providers (CSPs) dominate the global market — Amazon Web Services with a 29% market share, Microsoft with 20% and Google with 13%.[5] The Canadian market is similarly dominated by these same players, although there are few publicly disclosed numbers on its exact shape.

The so-called hyperscalers benefit from economies of scale. Our dependence can be weaponized in other ways as well. The American hyperscalers already make it difficult for clients to switch cloud providers, or use multiple different services at once, due to a lack of interoperability between their cloud environments, limited transparency and high egress fees.[6]

Sometimes, they even fail to provide export tools for migrating data in the first place, and anti-circumvention laws make it illegal for us to bypass these locks and reverse engineer our own data export tools.[7] Canada effectively has very little autonomy over its own data when it is in the hands of CSPs.

Moreover, in the context of American hyperscalers in particular, there are two U.S. laws that have important national security implications for Canadian data.

It is important to note that similar concerns would exist if Canadian cloud services were dominated by Chinese companies, or any other major geopolitical player. But we will focus on the United States in this paper, because that's the reality we live in.

The U.S. CLOUD Act

American companies are subject to the 2018 CLOUD Act ("Clarifying Lawful Overseas Use of Data Act") which asserts that U.S. law enforcement agencies can access data stored by U.S.-based companies, even when housed abroad.[8]

The CLOUD Act does not create broad surveillance powers, but instead applies quite narrowly to ongoing criminal investigations, and still requires warrants to be issued by an American court.

The CLOUD Act also preserves methods to challenge a warrant if it creates a conflict with the laws of another country.[9]

In the wake of the CLOUD Act coming into force, all the major CSPs emphasized that the law had little bearing on protections offered to customers.

Amazon states that the CLOUD Act "resulted in zero disclosures of AWS enterprise or government customer content stored outside the U.S. to the U.S. government, since [Amazon] started reporting the statistic in 2020"[10] and reports on the law enforcement information requests it receives.[11]

In a blog post about its data practices, Microsoft states that it "does not provide any government with direct and unfettered access to [its] customers' data [...nor…] with [the] encryption keys or the ability to break [their] encryption."[12]

In the FAQ section, it states that the CLOUD Act did not change its principles and customer commitments that relate to government requests for data. Microsoft publishes outcomes of requests it receives for customer data.[13] However, Microsoft also recently confirmed their powerlessness where the CLOUD Act is concerned. When asked by the French Senate whether it could guarantee that a French citizen's data would not be transmitted to U.S. authorities without the explicit authorization from French authorities, Microsoft's answer was no.[14] This admission confirms that data residency is not enough to guarantee sovereignty over Canadian data.

As *The Globe and Mail*'s Joe Castaldo and Pippa Norman point out, the number of law enforcement requests for data stored abroad might be fairly low. They report that Microsoft received a total of 5,560 information requests from American law enforcement, but only 52 warrants were for data stored abroad.[15]

The CLOUD Act also applies to Canadian companies that have a substantial enough presence in the U.S., meaning that even procuring from a Canadian company will not necessarily mean that data is protected from potential access by U.S. authorities.[16]

Foreign Intelligence Surveillance Act

The Foreign Intelligence Surveillance Act (FISA) is more problematic.[17] The government of Canada even identified FISA as the "primary risk" to data sovereignty, due to its potential for allowing the U.S. government to access Canadian information, without even notifying Canada.[18]

Specifically, Section 702 of FISA,[19] added in 2008, provides a legal framework for the U.S. to conduct surveillance of non-American persons located outside of the U.S. by compelling information, without requiring a warrant, from U.S.-based electronic communications providers, including CSPs.

The type of information to be collected is foreign intelligence information — loosely defined as information allowing the U.S. to protect itself against hostility from foreign governments.[20] Concerns have been raised over Section 702's potential for warrantless surveillance of the data of non-U.S. persons for "vague" national security reasons.[21]

Both FISA and the CLOUD Act represent obvious vulnerabilities to Canada's national security, but the United States has clearly signalled through multiple strategic documents that they see dominance in this space as a geopolitical imperative.

Sovereignty Washing

In spite of the CLOUD Act and FISA, the hyperscalers are positioning themselves as another option for sovereign cloud services in Canada. For example, Google recently announced its sovereign cloud offering for Canadian consumers.[22]

But critics have observed that Google and other hyperscalers are simply adapting their marketing strategies in recognition of the growing demand for sovereign cloud, by emphasizing data localization and robust security practices, while neglecting to mention their fundamental vulnerabilities.[23] In essence they are exploiting that there is no clear consensus on what sovereign cloud means.

Recent research from Upper Harbour finds that out of 715 of SaaS and Iaas tools used by Canadian organizations, 63% are parented in the U.S. and hence subject to the CLOUD Act.

Only 18% are Canadian-owned.

Out of the tools that offer Canadian data residency, often as a promise of sovereignty, 88% remain exposed to the CLOUD Act.[24] Another tactic that the hyperscalers are employing is to partner with local companies, which only complicates efforts to assess sovereignty.[25]

This tactic can also be observed in Canada: in December 2024, Cohere received $240 million in federal funding for its new data centre project, which it is building in partnership with U.S.-based CoreWeave.[26] This investment under the Sovereign AI Compute Strategy has attracted criticism for benefiting a U.S.-based company.[27]

Flying Blind

In September 2025, Prime Minister Carney said that his new Major Projects Office would be supporting the development of a Canadian sovereign cloud.[28]

The government has also been working on defining data sovereignty through research and white papers though requirements remain unclear.[29]

The Minister of AI and Digital Innovation, Evan Solomon, has been emphasizing the importance of building more Canadian infrastructure to achieve digital sovereignty. Minister Solomon has continued to implement the $2.4 billion package of measures to "secure Canada's AI advantage" including the Sovereign AI Compute Fund to increase Canadian-owned AI infrastructure.[30] However, in practice we see the pitfalls of rushing ahead with an infrastructure strategy without any clear governance strategy.

An initial investment under the Sovereign AI Compute Strategy has attracted criticism for primarily benefiting a U.S.-based company.[31]

While Canadian-based Cohere was the recipient of the funding, the money ultimately went to CoreWeave, an American company, to build infrastructure. Given CoreWeave's involvement, there are concerns that the data involved may ultimately be subject to the CLOUD Act and FISA.

Conclusion

The easiest way to think about Canada's digital infrastructure is by focusing on the data centres, the networking cables, and hard infrastructure. But as we've seen, the fixation on data residency and "sovereign" compute capacity fails to engage with the most important dimensions of the digital economy.

Canada must have a comprehensive governance strategy that meaningfully addresses data control, IP ownership, and the marketplace frameworks that shape the digital economy.

In the following chapters of *Foundations of Digital Sovereignty*, we will look into the ways that Canada can assert meaningful sovereign control over cloud systems and build up compute capacity for the benefit of Canadian companies. These policies will work in concert with a National Data Trust, an Innovation Asset Bank, and other policy ideas that we have already discussed in Chapters 1-4.

By taking a holistic approach, and taking inspiration from peer nations that are grappling with the very same policy challenges, we can move Canada along the spectrum toward more sovereign infrastructure.

Solutions

Canada needs to clearly understand the risks posed by our reliance on foreign hyperscalers and think strategically about what trade-offs to accept. There are several policy levers at our disposal for addressing and mitigating these risks:

1 The Canadian government should develop and adopt a procurement strategy that categorizes government data according to its sensitivity and assigns sovereignty requirements accordingly. For some use cases, procuring from American hyperscalers is appropriate, for others, we should procure from Canadian CSPs with limited or no presence in the U.S. to better protect data from foreign access.

2 Canada should adapt existing legislative and regulatory instruments to the cloud services market, including tools related to competition policy, blocking statutes, and utility regulation. Strengthened contractual obligations in procurement and a concerted effort to preserve our digital autonomy in trade agreements are other policy levers we can employ.

3 Canada should invest in the development of publicly-anchored digital infrastructure to create compute capacity for researchers, public service delivery and innovative Canadian businesses. Such investment will further broaden the suite of options available for compute requirements, and strategically fortify governance efforts.

References

1 Synergy Research Group, "Cloud Market Share Trends - Big Three Together Hold 63% while Oracle and the Neoclouds Inch Higher," November 19, 2025, https://www.srgresearch.com/articles/cloud-market-share-trends-big-three-together-hold-63-while-oracle-and-the-neoclouds-inch-higher.

2 Upper Harbour, "Independent research on Canadian data sovereignty," last updated Q1 2026, https://www.upperharbour.ca/research.

3 Stephanie Susnjara and Ian Smalley, "What is cloud computing?," IBM, accessed December 9, 2025, https://www.ibm.com/think/topics/cloud-computing; Calligo, "Understanding Cloud Service Models: SaaS vs. IaaS vs. PaaS," December 1, 2023, https://www.calligo.io/insights/glossary/understanding-cloud-service-models-saas-vs-iaas-vs-paas/; Microsoft, "What is cloud computing?," accessed December 9, 2025, https://azure.microsoft.com/en-us/resources/cloud-computing-dictionary/what-is-cloud-computing.

4 Government of Canada, "GC Cloud Framework Agreements Catalogue," GC Hosting Services Portal, accessed December 9, 2025, https://hosting-services-hebergement.canada.ca/s/gc-cloud-fa-catalogue?language=en_US.

5 Synergy Research Group, "Cloud Market Share Trends."

6 Songrim Koo and Connor Hogg, "Competition in the Provision of Cloud Computing Services," *OECD Roundtables on Competition Policy Papers*, no. 323 (2025), https://www.oecd.org/content/dam/oecd/en/publications/reports/2025/05/competition-in-the-provision-of-cloud-computing-services_f42582ad/595859c5-en.pdf; CMA, "Cloud Services Market Investigation: Summary of Final Decision" July 31, 2025, https://assets.publishing.service.gov.uk/media/688b20e6ff8c05468cb7b120/summary_of_final_decision.pdf.

7 Cory Doctorow, "Microsoft, Tear Down That Wall!," Medium, October 15, 2025, https://doctorow.medium.com/https-pluralistic-net-2025-10-15-freedom-of-movement-data-dieselgate-2ba103e567d1.

8 CLOUD Act, P.L. No. 115–141, Division V (2018), https://www.justice.gov/criminal/media/999391/dl?inline.

9 Michael Fekete and John Salloum, "Data sovereignty in light of the CLOUD Act: back to the future?," Osler, October 7, 2025, https://www.osler.com/en/insights/updates/data-sovereignty-in-light-of-the-cloud-act-back-to-the-future/#_ftn5.

10 Amazon, "Clarifying Lawful Overseas Use of Data (CLOUD) Act," accessed December 9, 2025, https://aws.amazon.com/compliance/cloud-act/.

11 Amazon, "Law Enforcement Information Requests," accessed December 9, 2025, https://www.amazon.com/gp/help/customer/display.html?nodeId=GYSDRGWQ2C-2CRYEF.

12 Microsoft, "About our practices and your data," accessed December 9, 2025, https://blogs.microsoft.com/datalaw/our-practices/#disclose-additional-data-CLOUD-act.

13 Microsoft, "Government Requests for Customer Data Report," accessed December 9, 2025, https://www.microsoft.com/en-us/corporate-responsibility/reports/government-requests/customer-data.

14 Sénat Français, "Audition de M. Anton Carniaux, directeur des affaires publiques et juridiques, et Pierre Lagarde, directeur technique du secteur public, de Microsoft France," Comptes Rendus de la CE Commande Publique, June 10, 2025, https://www.senat.fr/compte-rendu-commissions/20250609/ce_commande_publique.html.

15 Joe Castaldo and Pippa Norman, "Detangling Canadian Data," *The Globe and Mail*, October 17, 2025, https://www.theglobeandmail.com/business/technology/article-canada-data-centres-sovereignty-tech-companies-ai/.

16 Barry Appleton, " Whose Law Governs Canadian Data? The CLOUD Act, Executive Agreements, and Digital Sovereignty," New York Law School, Balsillie School of International Affairs, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=5955017.

17 Foreign Intelligence Surveillance Act of 1978, P.L. No. 95-511, 92 Stat. 1783, https://www.govinfo.gov/content/pkg/STATUTE-92/pdf/STATUTE-92-Pg1783.pdf.

18 Treasury Board Secretariat, "Government of Canada White Paper: Data Sovereignty and Public Cloud," published 2018, last modified October 31, 2025, https://www.canada.ca/en/government/system/digital-government/digital-government-innovations/cloud-services/digital-sovereignty/gc-white-paper-data-sovereignty-public-cloud.html.

19 Office of the Director of National Intelligence (U.S.), "FISA Section 702," Intel.gov, accessed December 9, 2025, https://www.intel.gov/foreign-intelligence-surveillance-act/fisa-section-702.

20 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.

21 Civo, "Is your cloud data truly sovereign? The CLOUD Act and FISA 702 reality check," July 24, 2025, https://www.civo.com/blog/is-your-cloud-truly-sovereign.

22 Farsad Nasseri and John Cousens, "Advancing Sovereignty, choice, and security in the cloud for our customers in Canada," Google, September 17, 2025, https://blog.google/intl/en-ca/products/supporting-businesses/advancing-sovereignty-choice-and-security-in-the-cloud-for-our-customers-in-canada/.

23 Aniket Patil, "Unveiling the Sovereign Cloud: Empowering the Public Sector in the Digital Age (Guest Blog from VE3)," TechUK, April 23, 2024, https://www.techuk.org/resource/unveiling-the-sovereign-cloud-empowering-the-public-sector-in-the-digital-age-guest-blog-from-ve3.html.

24 Upper Harbour, "Independent research on Canadian data sovereignty."

25 Patil, "Unveiling the Sovereign Cloud."

26 Josh Scott, "Cohere secures federal backing to build multibillion-dollar Canadian AI data centre," *Betakit*, December 6, 2024, https://betakit.com/cohere-secures-federal-backing-to-build-multibillion-dollar-canadian-ai-data-centre/.

27 Joe Castaldo, "Canadian Government Funding for AI development to benefit US company, critics note," *The Globe and Mail*, December 23, 2024, https://www.theglobeandmail.com/business/article-canadian-government-funding-for-ai-development-to-benefit-us-company/.

28 Alex Riehl, "Carney says new Major Projects office will help build a 'Canadian sovereign cloud'," *Betakit*, September 11, 2025, https://betakit.com/carney-says-new-major-projects-office-will-help-build-a-canadian-sovereign-cloud/.

29 Treasury Board of Canada Secretariat, "Government of Canada white paper: data sovereignty and public cloud," Government of Canada, June 25, 2018, 6, https://publications.gc.ca/site/eng/9.858956/publication.html.; Government of Canada, "Digital Sovereignty: A Framework to improve digital readiness of the Government of Canada," last modified November 12, 2025, https://www.canada.ca/en/government/system/digital-government/digital-government-innovations/cloud-services/digital-sovereignty/digital-sovereignty-framework-improve-digital-readiness.html#toc5.

30 Prime Minister's Office, "Securing Canada's AI advantage," Government of Canada, April 7, 2024, https://www.pm.gc.ca/en/news/news-releases/2024/04/07/securing-canadas-ai.

31 Castaldo, "Canadian Government Funding for AI development."