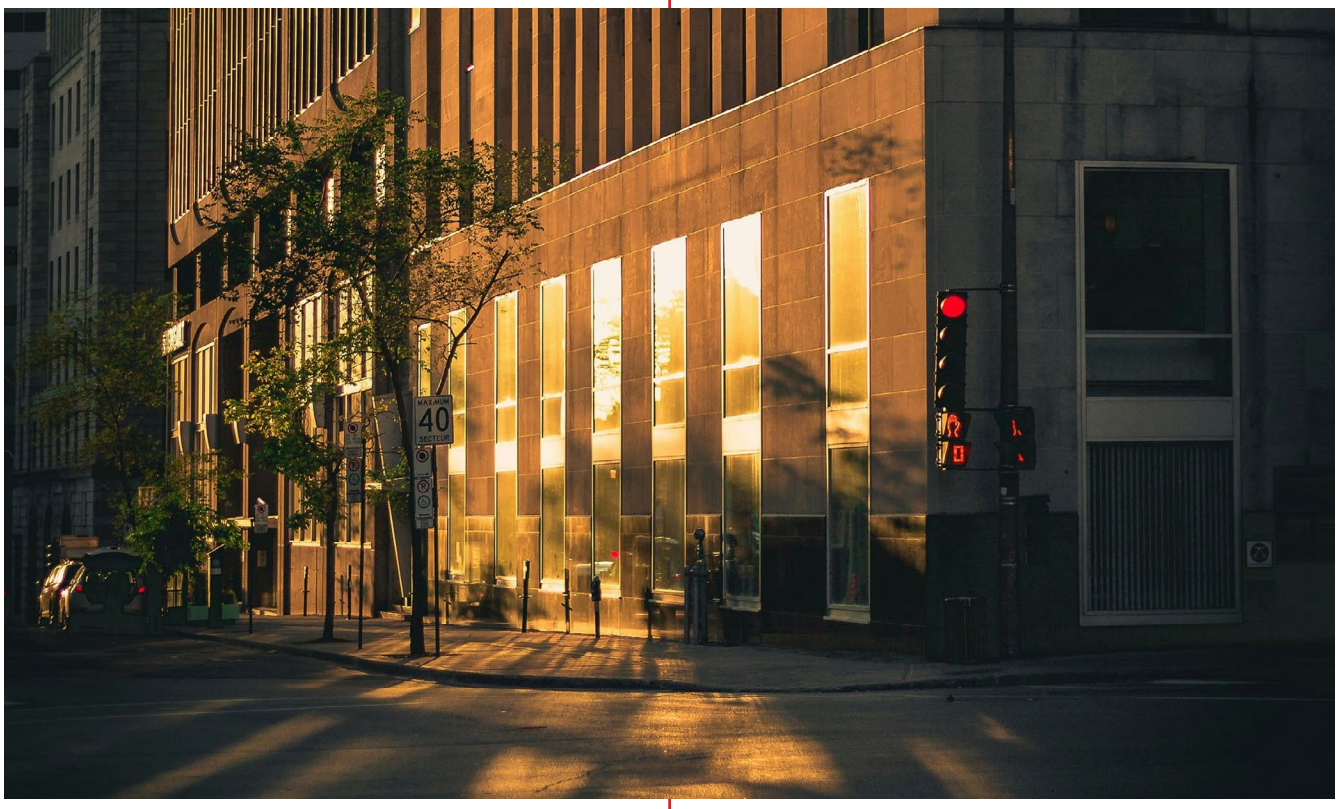
Back to Basics:
Using Existing Powers to Assert Digital Sovereignty

Canadian Shield Institute

Foundations of Digital Sovereignty
Chapter 7 - June 2026



7

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:

Alexandre St Louis
Scott Webb
Gene Dizon

Overview

Canada doesn't need to start from scratch to push back against foreign digital dominance. Many of the tools required to assert meaningful sovereignty already exist — they just need to be used more aggressively and strategically.

We look at four categories of existing policy levers: competition policy, public interest regulation, trade policy, and blocking statutes. Together, these tools can discipline hyperscaler behaviour, reduce vendor lock-in, and create the conditions for Canadian firms to compete — without waiting for new institutions to be built from the ground up.

Key Takeaways

1. The cloud services market is highly concentrated among a handful of foreign firms. Canada's Competition Bureau should conduct an in-depth study of the cloud market as a first step, with unbundling requirements and interoperability mandates as potential follow-on actions.

2. Hyperscalers could be regulated as public utilities — similar to how Canada regulates telecommunications providers — with obligations for transparent pricing, fair access, data portability, and interoperability.

3. Canada's existing trade agreements, including CUSMA, restrict our ability to privilege domestic firms and require data localization. However, all of Canada's trade agreements include a national security exception — invoking it and preserving it in renegotiations will be essential to protecting digital sovereignty.

Introduction

Digital sovereignty is not just a question of building Canadian alternatives to the dominant, foreign firms that currently mediate much of our digital economy.

Throughout *Foundations of Digital Sovereignty*, we have looked at the imperative for better governance over digital systems — through sovereign control of IP, technical standards, data usage, and through the physical cloud infrastructure that powers our digital experience.

Ultimately, the foundation of a prosperous and sovereign digital society rests upon public institutions and policy tools to meet the moment.

Canada has largely failed to recognize how the 21st century digital economy is a far departure from the production economy of the 20th century. This is why Canada needs to build institutions such as a national data trust and an innovation asset bank. But as we think about a comprehensive strategy for asserting sovereign governance over the digital economy, it's important to remember that it is still a dimension of the economy.

Many existing policy tools that were developed for shaping the economy for shared prosperity and public good are still relevant today. Digital platforms and hyperscaler multinationals may be extremely large businesses, but they are still businesses.

Competition Policy

In the digital realm, we see many examples of global markets dominated by just one or a handful of massive companies —i.e., hyperscalers. These companies can operate at a scale that makes the Canadian market seem small by comparison.

Take, for example, the cloud services market. As it stands, the cloud services market is highly concentrated among a handful of foreign cloud service providers (CSPs). Huge economies of both scale and scope have enabled Amazon, Google and Microsoft to create strong barriers to entry and expansion.[1] Addressing these issues from a standpoint of fair competition will directly support digital sovereignty by reigning in the power of dominant firms and giving our domestic CSPs a fighting chance.

Increased competition would also lead to better market outcomes more broadly, including more competitive prices, and improvements in quality and innovation. And because CSPs provide critical infrastructure, healthy and fair competition is even more imperative.[2] There are proposals and policy ideas for ways to break up hyperscaler CSPs,[3] however, this option requires a competition regulator both powerful enough and willing to undertake it. As a first step, Canada's Competition Bureau could conduct an in-depth study of the cloud services market in Canada to provide more powerful data and insight.

Where separation is not possible, there are other actions that can be taken to limit hyperscaler control. As an example, requirements for the unbundling of digital products across the tech stack may be one solution for the Canadian context.

As it currently stands, hyperscalers are best positioned to leverage bundled services and lock consumers into their products due to their economies of scope.

Interoperability is also necessary to promote fair competition. Data portability is especially important for empowering consumers and promoting more competition and innovation, as a study by the Competition Bureau found.[4]

The interoperability requirements proposed as part of modernized data legislation discussed in Chapter 5 would already go a long way in empowering consumers to switch easily between CSPs or using multiple different ones at once. Such arrangements are currently technically unfeasible due to barriers imposed by hyperscalers.[5]

Beyond these data rights, digital policy advocate Cory Doctorow has also proposed repealing anti-circumvention laws, which currently make it illegal to bypass digital locks implemented by operators and constrain data portability and interoperability, to support digital sovereignty efforts.[6]

Regulating for the Public Interest

In earlier generations of technology development, governments have grappled with policies to rein in the power of dominant firms. Some of these regulations could be applied to digital platforms, or adapted to a 21st century context.

One solution that emerges from the European context from a paper by the Open-Markets Institute is to classify cloud infrastructure as essential infrastructure, and implement a regulatory regime that treats cloud service providers as public utilities.[7]

Hyperscalers would face obligations to provide transparent, consistent pricing, fair and non-discriminatory access, interoperability and data portability, cybersecurity, resilience, privacy, and sustainability. Japan exemplifies this approach.

Japan's Cloud Program, under the Economic Security Promotion Act, classifies cloud services as critical products and subsidizes domestic services to reduce the dependence on foreign firms.[8] In Canada, the best analogy would likely be our regulation of telecommunication providers. The Wireless Code includes obligations for clear communication and contractual language from wireless providers, imposes limits on cancellation fees, and makes it easier to switch providers.[9]

The Internet Code places similar obligations on internet service providers, including requirements for easy to understand contracts and transparent pricing. These same obligations for CSPs could go a long way to address vendor lock-in and barriers to using multiple CSPs at once.[10]

Trade policy

Trade policy and international agreements are one tool by which Canada can advance our digital sovereignty. Unfortunately, our now existing trade agreements have mostly traded away Canada's ability to maintain sovereign governance over digital systems, in exchange for market access.

CUSMA's Digital Trade Chapter restricts Canada from privileging domestic firms.[11] Canada is also largely prevented from passing laws to require data localization, and under CUSMA we are not able to compel companies to provide source code for their technology, which then limits our ability to understand and regulate their services.

CUSMA includes requirements against discriminatory treatment for non-Canadian digital products. Through the WTO Agreement on Government Procurement, we are similarly committed to non-discriminatory treatment in government procurement.[12]

However, Canada's trade agreements all provide a carve-out through our national security exception, which states that nothing in an agreement can be construed to prevent the government from taking any action necessary for national security.[13]

Preserving, and invoking, the national security exception will be essential in Canada's efforts to secure our digital sovereignty.

Despite the clear national security argument for sovereign compute, the U.S. is unlikely to take kindly to any efforts contrary to the interests of its domestic firms. Indeed, in a recent U.S. Trade Representative Report, both Canada's Buy Canadian policy and Sovereign Cloud Initiative are listed as trade barriers.[14]

The current U.S. administration has also explicitly ordered its diplomats to lobby against digital sovereignty initiatives—presumably over fears of dismantling the dominance of American Big Tech.[15] Along with the 2025 National Security Strategy, these actions demonstrate a worrying convergence between interests of American tech firms and state power.[16]

Blocking Statutes

Blocking statues are instruments used specifically to counter the extraterritorial overreach of a foreign jurisdiction. They work by creating a clear conflict between the laws: For example, if a company receives a legally binding request from one country to hand over customer data, the blocking statute of another country would explicitly forbid handing over customer data to a foreign government.

Under the threat of potential prosecution, blocking statutes therefore will dissuade companies from complying with foreign requests for information, and may even deter foreign tribunals or bodies from making the request in the first place.

Canada has a blocking statute on the books in the form of the Foreign Extraterritorial Measures Act (FEMA),[17] however the law is poorly enforced and may not be broad enough to cover U.S. data requests under the CLOUD Act.[18]

To realize the potential value of a blocking statute, American case history makes clear that blocking statutes must be accompanied with diligent enforcement in order to be taken seriously.[19]

Otherwise, Canadian companies are likely to ignore their obligations under FEMA and instead comply with U.S. orders.

Technical Protections

Canada can assert greater control and governance over cloud compute and data storage through privacy-enhancing technologies, and contractual language in government procurement.

For example, when buying from foreign hyperscalers, the government can insist on technical protections like end-to-end encryption with customer-held keys for all data, which can substantially minimize the risks of foreign access to information.

Procurement contracts could also include obligations for CSPs to inform customers when they receive requests from foreign entities for access to information, or at least to provide their procedures for navigating conflicts between contractual requirements and foreign laws given such disclosure may sometimes be prohibited by U.S. law.

Canada can also explore other privacy-enhancing technologies. For example, "federated learning" is a technology specifically for AI training, where the training of an AI model happens on local devices, called edge computing, without handing over your data to the AI company itself. On-device, or edge computing in general, is a way to cut out the need for cloud computing in cases where that is possible.

Conclusion

Digital sovereignty will never be achieved through just one mechanism. It is not purely a procurement problem, just as much as it is not purely a competition problem.

Ultimately, digital sovereignty cuts across many different layers and therefore requires several different, yet complementary, efforts.

Canada benefits from the reality that many other countries are also grappling with questions of digital sovereignty, and we can explore a range of ideas that are being explored by peer jurisdictions. All the options presented above and in previous chapters are also mutually reinforcing. For example, increased transparency through more robust data governance could enable better tailored regulatory efforts.

With strong legislative and infrastructural foundations, we can make use of a suite of additional regulations, policies, and incentives to construct the necessary governance to build and protect Canadian digital sovereignty.

Solutions

Canada's existing policy toolkit is powerful but underused. To discipline hyperscaler behaviour and create the conditions for Canadian firms to compete, the Government of Canada should:

1. Direct the Competition Bureau to conduct an in-depth study of the cloud services market, with unbundling requirements and interoperability mandates as potential follow-on actions.

2. Introduce public utility regulation for cloud service providers, modelled on existing telecom obligations that require transparent pricing, fair access, data portability, and interoperability.

3. Invoke and preserve the national security exception in all existing and renegotiated trade agreements, establishing it as the legal foundation for any measures that privilege Canadian digital infrastructure.

4. Strengthen and actively enforce the Foreign Extraterritorial Measures Act, and assess whether it requires modernization to cover U.S. data requests under the CLOUD Act.

5. Embed technical protections, including end-to-end encryption with customer held keys — and disclosure obligations into all government procurement contracts with foreign cloud service providers.

References

1 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; Songrim Koo and Connor Hogg, "Competition in the Provision of Cloud Computing Services," *OECD Roundtables on Competition Policy Papers*, no. 323 (2025), https://doi.org/10.1787/20758677.

2 CMA, "Cloud Services Market Investigation."

3 Max von Thun and Claire Lavin, "Engineering the Cloud Commons," Open Markets Institute, May 2025, https://www.openmarketsinstitute.org/publications/report-rethink-regulatory-approach-to-essential-cloud.

4 Competition Bureau, "How data portability can unlock competition and empower consumers", Government of Canada, January 15, 2026, https://competition-bureau.canada.ca/en/how-we-foster-competition/education-and-outreach/publications/your-data-your-control.

5 CMA, "Cloud Services Market Investigation."

6 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.

7 von Thun and Lavin, "Engineering the Cloud Commons."

8 Atsushi Sumikawa, "Inside Japan's struggle to build sovereign AI," *Asia Times*, September 10, 2025, https://asiatimes.com/2025/09/inside-japans-struggle-to-build-sovereign-ai/.

9 Canadian Radio-television and Telecommunications Commission (CRTC), "Protected by the Wireless Code," Government of Canada, last modified February 17, 2026, https://crtc.gc.ca/eng/phone/mobile/code.htm.

10 CRTC, "The Internet Code: Protecting your rights," Government of Canada, last modified October 2, 2025, https://crtc.gc.ca/eng/internet/code.htm.

11 Government of Canada, "Canada-United States-Mexico Agreement (CUSMA) - Chapter 19 - Digital Trade," last modified July 31, 2020, https://www.international.gc.ca/trade-commerce/trade-agreements-accords-commerciaux/agr-acc/cusma-aceum/text-texte/19.aspx?lang=eng.

12 World Trade Organization, "Agreement on Government Procurement: Text of the Agreement," accessed April 16, 2026, https://www.wto.org/english/tratop_e/gproc_e/gpa_1994_e.htm.

13 Office of the Procurement Ombud, "Updated: National security exception," Government of Canada, last modified 2025, https://opo-boa.gc.ca/miseajour-esn-updated-nse-eng.html.

14 United States Trade Representative, *2026 National Trade Estimate Report on Foreign Trade Barriers of the President of the United States on the Trade Agreements Program*, February 28, 2026, https://ustr.gov/sites/default/files/files/Press/Releases/2026/National%20Trade%20Estimate%20Report%202026.pdf

15 Raphael Satter and Alexandra Alper, "Exclusive: US orders diplomats to fight data sovereignty initiatives," *Reuters*, February 25, 2026, https://www.reuters.com/sustainability/boards-policy-regulation/us-orders-diplomats-fight-data-sovereignty-initiatives-2026-02-25/.

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

17 Foreign Extraterritorial Measures Act, R.S.C., 1985, c. F-29, https://laws-lois.justice.gc.ca/eng/acts/f-29/index.html.

18 Barry Appleton, "Whose Law Governs Canadian Data? The CLOUD Act, Executive Agreements, and Digital Sovereignty," SSRN (Working Paper), December 22, 2025, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=5955017.

19 M.J. Hoda, "The Aérospatiale Dilemma: Why U.S. Courts Ignore Blocking Statutes and What Foreign States Can Do About It," *California Law Review* 106, no. 1 (2018): 231–261, https://www.jstor.org/stable/44630790.